Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)125

25.01.2023

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Antworten des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Fragenkatalog zur Öffentlichen Anhörung des Ausschusses für Digitales am 25.01.2023 „Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“

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?**

Antwort BSI: Das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Cyber-Sicherheitsbehörde des Bundes, begrüßt die Vorhaben des Koalitionsvertrages im Bereich der IT-Sicherheit ausdrücklich. Basierend auf seiner technischen Expertise antwortet das BSI wie folgt:

Ausbau des BSI zur zentralen Stelle der IT-Sicherheit des Bundes
Der im Koalitionsvertrag der Regierungskoalition beschlossene strukturelle Umbau der IT-Sicherheitsarchitektur ist aus Sicht des BSI dazu geeignet, das IT-Governance-Defizit des Bundes im Bereich der Informationssicherheit, sowohl in der Innenperspektive für die Eigensicherung der IT und Netze des Bundes, als auch in der Außenperspektive für das sichere Umsetzen und Unterhalten digitaler staatlicher Angebote für die Bürgerinnen und Bürger und die Wirtschaft zu adressieren.

Eine solide IT-Governance-Struktur – auch im Bereich der Informationssicherheit – ist dabei mehr als die Summe ihrer Teile. In Anbetracht der weiteren Entwicklung der Konsolidierung von IT-Infrastrukturen und zunehmender Abhängigkeit der Verwaltung von Technologie, muss die Bundesregierung ihre IT-Sicherheitskompetenzen künftig ressortübergreifend organisieren.

Aufbauorganisatorisch benötigt der Bund hiesigen Erachtens eine eigenständige zentrale Steuerungsinstanz, die den Gesamtüberblick über die IT-Sicherheitsrisiken seiner IT, aber auch seiner digitalen Angebote behält, daraus ein Gesamt-Risikoprofil erstellt und bei Bedarf im Wege des Informationssicherheitsmanagementsystems (ISMS) Bund steuernd eingreift.

Mit dem BSI hat die Bundesregierung bereits ein schlagkräftiges Kompetenzzentrum, welches diese notwendige Rolle mit wenigen aufbau- und ablauforganisatorischen Maßnahmen als zentrale Stelle mit seiner technisch tiefgehenden Expertise für den Bund einnehmen kann; insbesondere dann, wenn es in der Lage ist, unabhängig und ressortübergreifend zu agieren.

Die von der Regierungskoalition geplante unabhängigere Aufstellung des BSI, die notwendigerweise (insbesondere zur Wahrung eben jener unabhängigeren Aufstellung) mit der Übertragung der gesamtverantwortlichen Rolle des geplanten CISO Bund einhergehen muss, würde diesen Umständen Rechnung tragen und die Informationssicherheit als einen entscheidenden Faktor für die Zukunftsfähigkeit der IT-Governance-Struktur des Bundes substantiell stärken.

Ausbau des BSI zur Zentralstelle der IT-Sicherheit im Bund-Länder-Verhältnis:
Die übergreifende Gefährdungslage erfordert eine enge Verzahnung von Bund und Ländern im Bereich der Cyber- und Informationssicherheit sowie eine kooperative und komplementäre Ausgestaltung der Cybersicherheits-Architektur. Komplementär bedeutet in diesem Zusammenhang, dass Strukturen, Aufgaben und Schnittstellen klar definiert sein müssen und Doppelstrukturen vermieden werden sollten.
Da der derzeitige Rechtsrahmen in diesem Bereich bereits ausgeschöpft ist, hat das BSI gemeinsam mit dem BMI ein Konzept zum Ausbau des BSI zur Zentralstelle im Bund-Länder-Verhältnis erarbeitet. Ziel ist es, das BSI – neben dem BKA und dem BfV – zur dritten Säule einer föderal integrierten Cybersicherheits-Architektur auszubauen. Durch die intensivere Zusammenarbeit zwischen Bund und Ländern werden Ressourcen des Staates durch abgestimmtes Handeln und Bündelung von Kompetenzen effektiver eingesetzt und somit das Cybersicherheits-Niveau in Deutschland erhöht.

Unabhängigere Aufstellung des BSI:
Das BSI ist eine Behörde von besonderer Bedeutung, die für Exekutive, Legislative und Judikative als übergreifender Berater und Dienstleister in Angelegenheiten der IT-Sicherheit zur Verfügung steht (u.a. Corona-Warn-App, Smart Meter, Autonomes Fahren, Luftsicherheit, eIDs, etc.). Im Rahmen der IT-Konsolidierung sorgt das BSI für die Sicherheit der gesamten Bundes-IT sowie von Einrichtungen der Justiz, die eine verfassungsrechtlich garantierte Unabhängigkeit genießen. Für eine zielführende und vertrauensvolle Zusammenarbeit mit Exekutive, Legislative und Judikative in Fragen der Informationssicherheit ist es mit fortschreitender Digitalisierung essentiell, dass das BSI als fachlich unabhängige und kompetente Behörde wahrgenommen wird und seine Aufgaben allein auf Grundlage wissenschaftlich-technischer Erkenntnisse wahrnimmt. Mit einem unabhängigeren BSI erhöht sich auch das Vertrauen von Wirtschaft und Gesellschaft in dessen Angebote (u.a. IT-Grundschutz, Standardisierung und Zertifizierung, Beratungsleistungen für KMU etc.). Dies ist ein Gewinn für die Informationssicherheit Deutschlands. Näheres siehe Antwort auf Frage 2.

Keine Duplizierung und Zersplitterung der Zuständigkeiten:
Das BSI deckt bereits heute alle drei Säulen der Cyber-Sicherheit ab: Prävention, beispielsweise in der Zertifizierung von Produkten, Beratung, Erstellung von Standards und Richtlinien; Detektion, zum Beispiel im Rahmen des Schutzes der Regierungsnetze; Und Reaktion, beispielsweise bei der Vor-Ort-Unterstützung Kritischer Infrastrukturen durch die Mobile Incident Response Teams des BSI und dem Nationalen IT-Krisenreaktionszentrum des BSI. Zwischen Prävention, Detektion und Reaktion bestehen vielfältige Synergien, die das BSI nicht nur zugunsten der Ergebnisqualität nutzt, sondern auch zugunsten der Effizienz. Dopplungen und Fragmentierungen der Zuständigkeiten im Bereich der Cyber-Sicherheit gilt es daher zu vermeiden bzw. zu reduzieren.

Nationales IT-Lagezentrum und Nationales IT-Krisenreaktionszentrum des BSI:
Das Nationale IT-Lagezentrum des BSI ist das Herz der operativen Cyber-Abwehr Deutschlands. Als zentrale Meldestelle für IT-Sicherheitsvorfälle, Single Point of Contact für alle Zielgruppen des BSI und Lagebildersteller für die Cyber-Sicherheitslage in Deutschland, nimmt das Lagezentrum 24 Stunden am Tag und 7 Tage die Woche eine zentrale Rolle in der Sicherheitsarchitektur ein. In besonderen Fällen, zur Reaktion und Bewältigung von schweren Cyber-Sicherheitsvorfällen und IT-Krisen, wächst das Nationale IT-Krisenreaktionszentrum aus dem Nationalen IT-Lagezentrum und dem CERT-Bund heraus auf und bildet die Besondere Aufbauorganisation des BSI. Als Fach-Krisenstab analysiert und bewertet es die vorliegende Situation auf der Grundlage aller zur Verfügung stehenden Informationen und koordiniert alle weiteren beteiligten Krisenmanagementorganisationen, etwa der betroffenen Behörden, Dienstleister oder Kritischen Infrastrukturen.

Nationales Cyber-Abwehrzentrum:
Hinsichtlich des Nationalen Cyber-Abwehrzentrums empfiehlt das BSI, auch dort keine Dopplung von Cyber-Sicherheitsaufgaben vorzunehmen, sondern die ursprüngliche Zielsetzung des gegenseitigen Informationsaustausches, der Koordinierung von Aktivitäten und der „kurzen Wege“ bei der Abstimmung im Zuge der Vorfallsbewältigung zu verfolgen. Operative Aufgaben der Cyber-Sicherheit sollten hingegen bei den jeweils zuständigen Behörden verbleiben, die hierfür die notwendigen Rechtsgrundlagen haben bzw. erhalten. Auch nach einer Konsolidierung der Cyber-Sicherheitsaufgaben in der deutschen Cyber-Sicherheitsarchitektur wird eine gegenseitige Abstimmung von Aktivitäten unverzichtbar sein. Hierfür bietet sich das Nationale Cyber-Abwehrzentrum bzw. ein geeignetes Nachfolgeinstrument an.

Nationaler Cyber-Sicherheitsrat (NCSR):
Mit dem 2011 eingerichteten Nationalen Cyber-Sicherheitsrat (NCSR), in dem auch das BSI vertreten ist, verfügt die Bundesregierung über ein hochrangig besetztes Gremium, dem derzeit Vertreterinnen und Vertreter relevanter Bundesressorts, von Ländern, Kommunen und Wirtschaft angehören. Zudem berät eine ständige wissenschaftliche Arbeitsgruppe den NCSR aus Perspektive der Forschung. Der NCSR soll als Impuls- und strategischer Ratgeber zur Weiterentwicklung der Cyber-Sicherheit Deutschlands beitragen. Er bietet aufgrund seiner Scharnierfunktion zwischen den Akteuren die Möglichkeit einer umfassenden Perspektive auf die Cyber-Sicherheitslandschaft. In diesem Sinne hat der NCSR eine rein

beratende Funktion. Die Cyber-Sicherheitsstrategie (2021) sieht eine Weiterentwicklung des NCSR und eine Stärkung der ihm zugedachten Rolle als Impulsgeber vor.

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 herumgefragt: 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?**

Antwort BSI: Ziel muss es sein, die technisch-wissenschaftliche Entscheidungskompetenz des BSI zur Erfüllung seiner Aufgaben gemäß BSIG zu stärken. Dies wäre bereits durch einfachgesetzliche („BSI als selbstständige, fachlich unabhängige Bundesoberbehörde" im BSIG) und organisatorische Maßnahmen möglich, ohne dass fachaufsichtsfreie Räume entstünden. Demnach würde die Zusammenarbeit zwischen Fachaufsicht und BSI auf der Grundlage von jährlichen Zielvereinbarungen erfolgen, die eine Detailsteuerung und Ergebnisweisungen im Einzelfall ausschließen. Gewichtige politische Interventionen (z.B. politische Richtungsentscheidungen) blieben im Wege einer Ministergenehmigung möglich (analog zum BKartA). Zudem sollte eine direkte Zusammenarbeit des BSI mit allen Ressorts bei Digitalisierungsprojekten der jeweiligen Ressorts sowie eine direkte Zusammenarbeit des BSI mit den Ressorts und ihren Geschäftsbereichsbehörden, soweit es um deren Sicherheit und Schutz geht, ermöglicht werden. Hier ist eine Änderung in §26 GGO notwendig. Darüber hinaus siehe auch Antwort zu Frage 1.

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?**

Antwort BSI: Der von Prof. Dr. Waidner (ATHENE) und Frau Prof. Dr. Shulman (ATHENE) verfasste Gastbeitrag in der Frankfurter Allgemeinen Zeitung vom April 2022 bietet aus BSI-Sicht eine gute Basis zur Auseinandersetzung mit dem Thema. Entscheidend ist hierbei, dass aktive Cyber-Abwehr nicht mit einem „Hackback“ im Sinne eines Gegenschlages verwechselt wird. Mit § 7b Abs. 4, § 7c („Anordnungen des Bundesamtes gegenüber Diensteanbietern") und § 7d BSIG („Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten“) hat das BSI bereits verschiedene Eingriffsbefugnisse. Zielsetzung aktiver Cyber-Abwehr ist es nicht, Schaden beim Angreifer auszulösen, sondern – wie der Name bereits impliziert – Angriffe abzuwehren. Waidner und Shulman beschreiben vier Arten von aktiven Maßnahmen.

- Erstens können bestimmte Cyber-Angriffe dadurch gestoppt oder abgeschwächt werden, dass Veränderungen am Internet-Verkehr vorgenommen werden. Ein Beispiel hierfür sind kurzfristige Konfigurationsänderungen an den Routen des Datenverkehrs im Internet, mit denen bestimmte Angriffsformen unwirksam gemacht werden können.
  Mit dem IT-SiG 2.0 hat das BSI bereits in § 7c Abs. 1 S. 1 Nr. 1 BSIG i.V.m. § 169 TKG eine Befugnis bekommen, um TK-Provider unter bestimmten Rahmenbedingungen anzuweisen, den Datenverkehr von oder zu Angreifern umzuleiten oder zu blockieren. Zielrichtung der Umleitungs-Regelung in § 169 TKG ist der Schutz der IT von TK-Providern und Nutzern von IT-Systemen sowie vor dem Abfluss von Daten an Systeme der Angreifer. Dabei darf das BSI nur bei konkreten und erheblichen Gefahren tätig werden und muss zuvor das Einvernehmen mit der BNetzA herstellen.
- Die zweite Art von Maßnahmen ist die Übernahme oder Veränderung von Netzwerk-Ressourcen, auf die Angreifer bei ihren Aktivitäten zurückgreifen. Angreifer kapern oder infiltrieren beispielsweise oft legitime Systeme, etwa Server von Online-Shops, um diese Systeme für ihre Angriffe zu missbrauchen oder um ihre eigenen Aktivitäten zu verschleiern. In solchen Fällen können Cyber-Angriffe oft dadurch gestoppt oder geschwächt werden, dass diese Ressourcen den Angreifern entzogen werden.
  Das BSI darf die Netzwerk-Ressourcen – also etwa Server – nicht selbst übernehmen. Allerdings kann es nach § 7c Abs. 1 S. 1 Nr. 1 BSIG i.V.m. § 169 TKG anordnen, den Angriffs-Datenverkehr, der von diesen missbrauchten Netzwerk-Ressourcen ausgeht, umzulenken oder zu blockieren, um die angegriffenen Systeme zu schützen. Faktisch werden den Angreifern die Ressourcen dadurch ebenfalls entzogen, da sie keinen Kontakt zu den angegriffenen oder für Angriffe missbrauchten Systemen mehr herstellen können. Das BSI kann den Datenverkehr der Angreifer- oder der Opfersysteme auch gem. § 7c Abs. 3 und Ab. 4 BSIG auf eigene Systeme umleiten lassen, um diesen zu analysieren und Informationen über Schadprogramme oder das Vorgehen der Angreifer zu erhalten. Oftmals ist das BSI auch ohne förmliche Nutzung der Befugnis bereits erfolgreich, wenn es die entsprechenden Informationen an die Internetzugangsprovider weitergibt. Diese dürfen die entsprechenden Maßnahmen schon länger umsetzen, als es die BSI-Anweisungsbefugnis gibt und kooperieren in vielen Fällen, da sie ein Eigeninteresse an der Bereinigung bzw. Abschaltung der für Angriffe missbrauchten Systeme haben.
- Wenn Erkenntnisse darüber vorliegen, dass ein Cyber-Angriff bestimmte Schwachstellen auf sehr vielen betroffenen Systemen ausnutzt, kann die aktive Abwehr auch darin bestehen, diese Schwachstellen automatisiert auf den betroffenen Systemen zu beheben. Eine ähnliche Option ist es, Schadprogramme von einer großen Anzahl betroffener Systeme automatisiert zu entfernen. Dies ist die dritte von Waidner und Shulman dargestellte Kategorie aktiver Maßnahmen. Diese Vorgehensweise käme insbesondere dann in Betracht, wenn eine manuelle Behebung der Schwachstelle bzw. eine manuelle Desinfektion auf allen betroffenen Systemen zu aufwändig wäre.

Mit dem IT-SiG 2.0 hat das BSI in § 7 Abs. 1 S. 1 Nr. 2 BSIG eine entsprechende Befugnis zur Anweisung der TK-Provider erhalten. Es kann diese zur Verteilung von technischen Befehlen zur Bereinigung von einem konkret benannten Schadprogramm an die Nutzersysteme verpflichten. Zur Nutzung der Befugnis muss das BSI zuvor das Einvernehmen mit der BNetzA und dem BfDI herstellen.

- Als vierte Kategorie ist schließlich noch der Eingriff in die von den Angreifern genutzten Komponenten zu nennen. Solche Eingriffe können nicht nur dazu dienen, einen laufenden Angriff zu stoppen, sondern beispielsweise auch dazu, Informationen über die Angriffsmethoden oder die potenziellen Betroffenen von geplanten Angriffen zu gewinnen und dadurch die Prävention zu verbessern.
  Das BSI darf bisher nicht in IT-Systeme von Angreifern eindringen. Aber das BSI kann schädlichen Datenverkehr seit dem IT-SiG 2.0 gem. § 7c i.V.m. § 169 TKG durch entsprechende Anordnungen gegenüber den TK-Anbietern umleiten, blockieren oder analysieren. Zudem sind die TK-Anbieter bereits seit langem gem. § 169 Abs. 5 TKG verpflichtet, ihre Nutzer vor konkreten erheblichen Gefahren zu warnen und sie über Beseitigungsmaßnahmen zu informieren. Die Aspekte der Gefahrenabwehr, der Nutzerinformation aber auch der weiteren Informationsgewinnung sind also bereits gesetzlich geregelt, ohne dass dafür Gegenmaßnahmen im Sinne eines Hackbacks nötig wären.

Aus Sicht des BSI kommt aktive Cyber-Abwehr i.S von „Hackbacks“ nur in Betracht, wenn dafür eine explizite Rechtsgrundlage geschaffen wird, wenn es um die Abwehr besonders schwerwiegender Schäden geht, wenn weniger invasive Maßnahmen nicht zum Ziel führen und wenn im Rahmen einer sorgfältigen Risikoabschätzung die Gefahr unerwünschter Seiteneffekte eindeutig gegenüber den Chancen der Schadensbegrenzung durch solche Maßnahmen in den Hintergrund rückt. Unter Berücksichtigung dieser Randbedingungen wäre es wünschenswert, dass das bestehende Instrumentarium der defensiven Maßnahmen in herausgehobenen Fällen um aktive Maßnahmen (gemäß der oben beschriebenen Definition) der Cyber-Abwehr ergänzt wird.

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?

Antwort BSI: Das BSI begrüßt die Umsetzung aller obenstehenden Instrumente und Maßnahmen ausdrücklich. Alle genannten Aspekte sind wichtige Bausteine für einen präventiven Umgang mit IT-Sicherheit. Eine pauschale Priorisierung einzelner Maßnahmen erscheint aus Sicht des BSI nicht zielführend und auch nicht aus technisch-wissenschaftlichen Betrachtungen ableitbar.

Auswirkungen des Cyber Resilience Act:
Für Produkte mit einem erhöhten IT-Sicherheitsrisiko ist eine Bewertung bzw. Zertifizierung durch akkreditierte Stellen durchzuführen, wie dies beispielsweise im Entwurf des vorliegenden Cyber Resilience Act (CRA) der EU vorgesehen ist. Hierdurch soll sichergestellt werden, dass der Hersteller eines Produktes eine Risikobewertung durchgeführt und angemessene Sicherheitsfunktionen entwickelt und mit der notwendigen Sorgfalt implementiert hat. Ergänzend enthält der Cyber Resilience Act nicht nur die Verpflichtung Sicherheitslücken zu melden, sondern auch umgehend durch ein Update zu schließen. Neben dem Schwachstellenmanagement adressiert der Cyber Resilience Act auch die Instrumente Security-By-Design/-Default und das Recht (bzw. die Pflicht) zur Verschlüsselung und Integritätssicherung, sowie eine Reihe von weiteren sogenannten „Wesentlichen Anforderungen" an die Cybersicherheit von Produkten und damit verbundenen Diensten.

Darüber hinaus ist anzumerken, dass Cybersicherheit nicht nur in Produkten verankert werden muss, sondern auch in organisatorische Maßnahmen bzw. Prozesse integriert werden muss. Insbesondere müssen gesetzliche Verpflichtungen für den Einsatz von Informationssicherheitsmanagementsystemen (ISMS) wie beispielsweise den BSI-Grundschutz geschaffen werden. „Bug Bounty Programme" sollten im öffentlichen Bereich als organisatorische Maßnahme mit standardisierten Prozessen grundsätzlich genutzt werden, um so Anreize zu schaffen, Fehler der im öffentlichen Bereich genutzten Software und Hardware rechtssicher zu identifizieren und zu melden.

Produkthaftung:
Soweit es um Produkthaftung geht, kann diese sicherlich ein Instrument sein, um die Hersteller und Vertreiber zu einer besseren Absicherung der IT-Produkte zu bewegen.

Diesbezüglich gibt es inzwischen eine Reihe von Regulierungsvorhaben auf europäischer Ebene, die das Feld adressieren, so dass ein Tätigwerden des deutschen Gesetzgebers derzeit nicht nötig und wohl auch nicht sinnvoll möglich ist.

IT-Sicherheitsforschung:
IT-Sicherheitsforschung ist ein wichtiger Baustein, um auf neuen Entwicklungen basierende innovative IT-Sicherheitsverfahren auszuarbeiten. IT-Sicherheitsforschung trägt dazu bei, das Sicherheitsniveau in Deutschland zu erhöhen und Bürgerinnen und Bürger, Unternehmen und den Staat vor Angriffen präventiv und nachhaltig zu schützen und die Wettbewerbsfähigkeit des Standorts Deutschland zu stärken.

Deutschland verfügt im Bereich IT-Sicherheit über eine exzellente Forschungslandschaft aus international hoch anerkannten Gesellschaften, Instituten und Forschungsclustern der Hochschulen. Dennoch besteht eine Gefahr, dass wir im internationalen Vergleich abgehängt werden. Hauptgrund ist die immer schnellere Verbreitung der Digitalisierung in allen Lebensbereichen und die damit einhergehenden wachsenden Schutzbedarfe und zunehmenden Risiken. In dem Maße, wie die Bedrohungen im Cyberraum zunehmen, muss auch noch stärker in IT-Sicherheitsforschung und -entwicklung investiert werden.

Notwendig ist eine frühzeitige Einbindung der IT-Sicherheit als integraler Bestandteil in Technologieentwicklungen, wodurch Rahmenbedingungen zur Herstellung vertrauenswürdiger Technologien geschaffen und gleichzeitig nationale technologische Kompetenzen gestärkt werden. Schlussendlich muss der Transfer in die nationale Wirtschaft gewährleistet sein, um die Wertschöpfungskette für die geförderten Technologien durch die Bereitstellung marktfähiger Produkte hoher Vertrauenswürdigkeit zu erweitern.

IT-Sicherheitsforschende sehen für ihre Arbeit durchaus oft rechtliche Risiken durch unklare Strafvorschriften (z.B. der Hackerparagraf § 202c StGB) oder die Drohungen mit rechtlichen Schritten durch die Anbieter von IT-Produkten in denen sie Lücken entdeckt haben. Für das BSI wurden z.B. für die Untersuchung von Produkten auch erst mit dem IT-Sicherheitsgesetz 1.0 die Befugnisse geschaffen, mit denen die rechtlichen Risiken adressiert und Rechtssicherheit für das BSI erreicht werden konnte. Für IT-Sicherheitsforschende außerhalb des BSI fehlt es daran, obwohl gerade durch die große Menge an IT-Sicherheitsforschern viele Lücken und Risiken in Hard- und Software entdeckt werden. Daher wäre es sinnvoll, einen entsprechend sicheren Rechtsrahmen für die IT-Sicherheitsforschung zu schaffen. So kann das entsprechende Potenzial zur Entdeckung von Risiken für die Informationssicherheit besser genutzt werden. Für tiefergehende Informationen bietet sich ein vom Fraunhofer Institut für Informatik und anderen erstelltes Whitepaper an. (https://www.fzi.de/2021/11/25/dringender-reformbedarf-in-deutschland-whitepaper-zur-rechtslage-der-it-sicherheitsforschung/).

Open Source:
Die grundsätzliche Fördermöglichkeit von Open Source Software (und Hardware) durch die öffentliche Hand sollte gesetzlich explizit festgeschrieben werden. Die Verwendung von öffentlichen Finanzmitteln zur Produktion von Ergebnissen, die neben der öffentlichen

Verwaltung ohne rechtliche Hürden durch Bürger, Wirtschaft und Forschungsinstitutionen nutzbar sind, macht staatliches Handeln in diesem Bereich transparent und gewährt den Steuerzahlern einen unmittelbaren Nutzen. Die Vergabe von Projekten zur Förderung von Open Source Software ist derzeit im Vergleich zu Vergaben an Hersteller proprietärer Software erschwert und erfordert oftmals eine Begründung des Einzelfalls. Durch eine geeignete gesetzliche Grundlage könnte die Förderung von Open Source Software gestärkt werden.

Künstliche Intelligenz (KI):
Hinsichtlich des Einsatzes von Künstlicher Intelligenz (KI) sind folgende Aspekte von Bedeutung:

- (Offene) Standards für KI-Systeme stehen für Qualität, sorgen für Sicherheit und schaffen Vertrauen in KI. Sie ermöglichen Unternehmen einen besseren Zugang zu nationalen und internationalen Märkten.
- National und international (DIN, CEN/CENELEC, ETSI, ISO etc.) wird derzeit an der Entwicklung KI-spezifischer Standards gearbeitet. Das BSI arbeitet in den oben genannten Gremien aktiv mit.
- Ein wichtiger Arbeitsschritt ist dabei die Entwicklung der Prüfgrundlagen (Prüfkriterien, Prüfmethoden, Prüfwerkzeugen) zur Prüfung von KI-Systemen. Dies ist zum Teil noch Gegenstand der aktuellen Forschung.

Aus BSI-Sicht wichtige Maßnahmen:

- Entwicklung der Prüfgrundlagen für resiliente und vertrauenswürdige KI-Systeme. Deutschland arbeitet bereits an der Entwicklung der Prüfgrundlagen, beispielsweise:
    - Normungsroadmap KI (Ausgabe 1 und 2),
    - Leuchtturmprojekte der Normungsroadmap KI,
    - AI Cloud Service Compliance Criteria Catalogue (AIC4),

  Diese Aktivitäten sollen verstärkt werden.
- Aktive Beteiligung bei der Entwicklung von internationalen KI-Standards (diese Standards werden jetzt! erarbeitet), um dort
    - europäische Werte und Regeln zu verankern,
    - Bedarfe deutscher und europäischer Unternehmen einzubringen, um ihnen einen besseren Zugang zu internationalen Märkten zu ermöglichen.
- Förderung des Aufbaus eines europäischen Ökosystems für KI.

Defizite in Deutschland/EU:

- Marktbeherrschende Unternehmen, die KI-Dienstleistungen anbieten, kommen aus den USA und China.

Zu dem Punkt Schwachstellenmanagement/Meldung von Sicherheitslücken wird auf die Antwort zu Frage 7 verwiesen.

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?**

Antwort BSI: Siehe Antwort auf Frage 3.

Sowohl im Hinblick auf die Rechtsmäßigkeit als auch die Zweckmäßigkeit ist es sinnvoll, zwischen offensiven und aktiven Möglichkeiten zu differenzieren. Denn nicht jede aktive Maßnahme ist zwangsläufig auch offensiv. So hat das BSI etwa seit dem IT-Sicherheitsgesetz 2.0 die Befugnis, Anbieter zu Eingriffen in den Datenverkehr zu verpflichten, um Angriffe und Datenabflüsse zu verhindern bzw. zu beenden. Dabei handelt es sich um eine aktive Maßnahme, die jedoch nicht offensiv ist. Sie erlaubt zielgerichtet, den Angriffsverkehr, der von fremden Systemen ausgeht, zu blocken und damit Angriffen bereits auf Netzebene ein Ende zu setzen. Ein offensiver Eingriff auf den Systemen Dritter ist damit unnötig. Gleichzeitig wird das Risiko von Kollateralschäden durch Eingriffe in die Technik auf den Systemen Dritter ausgeschlossen. Da die Eingriffe auf Netzebene (eben durch Anweisung der Provider) stattfinden, können sie auch bei Angriffen aus fremden Staaten eingesetzt werden, ohne juristisch problematische Maßnahmen auf Systemen in fremden Staaten durchführen zu müssen. Damit wird ein wesentliches Problem von Hackbacks, nämlich die völkerrechtliche Zulässigkeit von Maßnahmen auf Systemen im Hoheitsgebiet anderer Staaten, umgangen.

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?**

Antwort BSI: Deutschland (hier BMI/BSI) tauscht sich regelmäßig mit vielen internationalen Stellen zu Fragen der Cybersicherheit aus. Sei es in multilateralen und institutionellen Formaten, etwa im EU- und NATO-Kontext, sei es in vielen bilateralen Kontakten. Dies ist auch deshalb bedeutsam, da Deutschland zunehmend europäischer Regulierung unterworfen ist und bei der Umsetzung ähnlichen Herausforderungen wie unsere Partner begegnet.

Dabei werden einerseits Erkenntnisse zu operativen Aspekten wie aktuelle technische Erkenntnisse geteilt (bspw. Ansätze der Detektion und Abwehr, Technologietrends, Instrumente und Konzepte der Informationssicherheit). Andererseits wird in vielen Dialogformaten und formalen Gremien über strategische und Policy-Fragen gesprochen: Es werden Erfahrungen zu jeweiligen nationalen Gesetzgebungen und Cyber-Sicherheitsstrategien geteilt und verglichen. Hieraus kann auf allen Ebenen – rein technisch; gestaltend mit Blick auf Instrumente und Kapazitäten; die ministerielle Ebene – geprüft und identifiziert werden, an welchen Stellen Deutschlands Cybersicherheit justiert werden sollte

und welche Best-Practices dafür aus dem Ausland herangezogen werden können. Dies ist aber natürlich keine Einbahnstraße. Als eine der führenden Cybersicherheitsbehörden in Europa unterstützen wir mit unserer Expertise auch unsere Partner und tragen so zu einem insgesamt höheren Maß an Cybersicherheit bei.

Mit Blick auf staatliche Stellen und Cyber-Sicherheits-Governance sind folgende Beispiele zu nennen: Cyber-Sicherheit wird international zunehmend als „Chefinnensache“ bzw. „Chefsache“ verstanden und das BSI beobachtet, dass Cyber-Sicherheitsbehörden in einigen Ländern direkt beim Premierminister angesiedelt sind. Auch genereller betrachtet gibt es die Tendenz zur zunehmenden Zentralisierung der Zuständigkeiten für Cybersicherheit. Aktuelle Beispiele hierfür sind die im Oktober 2022 veröffentlichte neue Cyber-Sicherheitsstrategie der Niederlande, in der die Gründung einer zentralen Behörde für Cybersicherheit angekündigt wird, sowie die Mitte 2021 erfolgte Gründung der Agenzia per la Cybersicurezza Nazionale (ACN) in Italien. Das BSI hat für eine Reihe von europäischen Partnerbehörden, etwa auch für die französische Partnerbehörde Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI), Vorbildcharakter hinsichtlich Strukturen und Zuständigkeiten.

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“)?**

Antwort BSI: Bevor überhaupt gesetzliche Regelungen zum staatlichen Umgang mit Schwachstellen geschaffen werden können, ist es hiesigen Erachtens notwendig, die Ziele, Definitionen und Rahmenbedingungen eines geplanten Schwachstellenmanagements festzulegen. So ist, rein auf Basis der Aussagen des Koalitionsvertrages, nicht klar, ob es sich bei dem Konzept um eine Art Coordinated Vulnerability Disclosure (CVD-Prozess), eine Art Vulnerabilities Equities Process (VEP), oder um beides inklusive darüberhinausgehender Maßnahmen handelt.

Grundsätzlich hat ein Schwachstellenmanagement, sofern es Zero Days behandelt, immer das Ziel, sie zu schließen. Um dies zu ermöglichen, müssen Sicherheitslücken stets an den Hersteller des betroffenen Systems gemeldet werden, denn nur er kann die Lücke mittels eines Patches schließen (kurzfristige „work arounds" ausgenommen).

Die entscheidende zu beantwortende Frage für den staatlichen Umgang mit Sicherheitslücken ist also nicht ob, sondern ob „direkt" oder „verzögert" an den Hersteller gemeldet wird und was in der Zwischenzeit mit der Lücke passiert. Während der CVD des BSI hier das Ziel einer direkten Meldung an den Hersteller verfolgt, ist ein bislang lediglich in anderen Staaten implementierter VEP dafür geeignet, im Wege einer Risikobewertung zu entscheiden, ob eine temporäre Nichtmeldung möglich ist, damit die Lücke zum Zwecke der Gefahrenabwehr, Strafverfolgung oder Aufklärung eingesetzt werden kann. Mit der im Koalitionsvertrag vorgenommenen Einschränkung durch die Begrifflichkeiten „nicht offenhalten" sowie „schnellstmögliche Schließung" wäre also ein CVD-Prozess die richtige

Wahl. Da jedoch ein CVD-Prozess im BSI existiert und gelebte Praxis ist, geht das BSI davon aus, dass die Regierungskoalition doch eher eine Art VEP meint. Durch die begriffliche Einschränkung würde der Umgang mit Lücken im Rahmen eines solchen VEP jedoch faktisch auf die Bewertung von N-Days reduziert.

Da ein Großteil der für bekannte Cyberangriffe ausgenutzten Sicherheitslücken N-Days sind/waren, ist eine strukturierte Risikobewertung vor dem operativen Einsatz durch Sicherheitsbehörden hiesigen Erachtens dabei durchaus sinnvoll. Zero Days würden in diesem Modell neben dem VEP parallel dem CVD für eine direkte Unterrichtung des Herstellers zugeleitet und somit zu „frühen N-Days“. Die im Koalitionsvertrag vorgesehene Federführung des BSI wäre ohne gesetzliche Änderungen im BSIG möglich, der grundgesetzliche Zielkonflikt zwischen IT-Sicherheit und öffentlicher Sicherheit wäre im Hinblick auf den staatlichen Umgang mit Schwachstellen gelöst.

Die Pflichten des Staates zum Schutz der unterschiedlichen Grundrechte führen im Kontext der IT-Sicherheit und öffentlichen Sicherheit, wie am staatlichen Umgang mit Zero-Days deutlich wird, in einen Zielkonflikt staatlicher Sicherheitspolitik und damit innerhalb der Cybersicherheitsarchitektur Deutschlands, qua unterschiedlicher gesetzlicher Aufträge, auch zu einem Interessenkonflikt zwischen dem BSI und den Sicherheitsbehörden.

Aus BSI-Sicht ist für ein staatliches Schwachstellenmanagement im Sinne eines VEP grundsätzlich entscheidend, ob ein solcher Prozess diesen Ziel- und Interessenkonflikt zum größtmöglichen Nutzen für die Informationssicherheit auflösen kann, wie er dafür entsprechend ausgestaltet werden und welche Bedingungen er dafür erfüllen muss. Um diese politische und gesetzgeberische Entscheidung zur Auflösung des grundrechtlichen Konflikts treffen zu können, ist es hiesigen Erachtens notwendig, die Erforderlichkeit und Verhältnismäßigkeit des Einsatzes von Zero Days durch Sicherheitsbehörden empirisch zu belegen. Auch die alternativen Möglichkeiten der Sicherheitsbehörden sind durch einen strukturierten Ansatz (etwa eine Inventarisierung der Instrumente) in die Entscheidung einzubeziehen (bspw. im Wege einer Überwachungsgesamtrechnung).

Darauf aufbauend ließen sich dann die technischen, personellen und organisatorischen Voraussetzungen eines staatlichen Umgangs mit Schwachstellen herausarbeiten.

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?**

Antwort BSI: Das BSI und das BBK arbeiten beim Thema Kritische Infrastrukturen seit vielen Jahren eng zusammen, sei es in der öffentlich-privaten Partnerschaft UP KRITIS, im bilateralen Austausch, bei der Umsetzung des 1. IT-Sicherheitsgesetzes oder im Cyber-Abwehrzentrum. Dabei sind uns die teilweise Überschneidung von physischem und IT-Schutz sowie die gleichartigen Auswirkungen bei Störungen stets bewusst.

Folgende Ansatzpunkte können bei der Ausgestaltung des KRITIS-Dachgesetzes eine wichtige Rolle spielen:

Identifizierung:
In Deutschland existiert mit dem BSIG und der BSI-KritisV eine effektive Identifizierung von Kritischen Infrastrukturen auf Bundesebene. Die dortige Identifizierung geschieht NICHT mit einem IT-Fokus, sondern identifiziert KRITIS-Betreiber im Hinblick auf deren Relevanz für die Versorgung der Bevölkerung und somit auf Basis einer allgemeinen Methodik, wie sie auch vom BBK in der Veröffentlichung „Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten“
(https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-20-schutz-infrastrukturen-identifizierung.pdf?__blob=publicationFile).
beschrieben wird. Die Methodik ist etabliert, akzeptiert und über Jahre erprobt und weiterentwickelt worden. Bei der Umsetzung der CER-Richtlinie sollte diese bestehende und wichtige Säule der bisherigen KRITIS-Regulierung, die eben gerade klärt, wer die Adressaten der Regulierung sind, bestmöglich erhalten bleiben, auch um Rechtssicherheit für die Betreiber zu schaffen und keine Inkonsistenzen zwischen der Regulierung des physischen Schutzes und des IT-Schutzes zu schaffen.

Aufsichtsrollen:
Das BSI hat sich in den vergangenen sieben Jahren als Aufsichtsbehörde über die Informations- und Cyber-Sicherheit Kritischer Infrastrukturen etabliert und diese Funktion erfolgreich wahrgenommen, mit Blick auf Kritische Infrastrukturen aller Sektoren. Das Verwaltungshandeln hat zudem gezeigt, dass eine Überschneidung vieler Zuständigkeiten unterschiedlicher Behörden die dringend gebotene Eile bei der Umsetzung aufsichtsrechtlicher Maßnahmen behindert. Die zentrale Rolle des BSI sollte in Zukunft, gerade auch im Zuge der Umsetzung der NIS-2-Richtlinie, beibehalten bzw. noch weiter ausgebaut werden. Es ist daher dringend zu empfehlen, Zuständigkeiten bzgl. zentraler Aspekte der Regulierung, wie beispielsweise der Informations- und Cyber-Sicherheit, an einer Stelle zu konzentrieren und, wo immer möglich, auf spezialgesetzliche Regelungen zu

verzichten, welche die Zuständigkeiten und Vorgehensweisen der verschiedenen Behörden deutlich komplexer, undurchsichtiger und letztlich weniger schlagkräftig machen. Gerade für das Thema Informations- und Cyber-Sicherheit bei KRITIS sollte es nur eine zuständige Behörde auf Bundesebene geben, das BSI. Das BSI kann die gewonnenen Erfahrungen zudem nutzen, um diese in den neuen Regulierungsaufgaben bzgl. physischer Sicherheit einzubringen. Eine ganz enge Zusammenarbeit mit dem BBK scheint hier vorteilhaft, um die sich überschneidenden Bereiche aus verschiedenen Blickrichtungen bestmöglich zu bearbeiten.

Sensitive Daten:
Beim Verwaltungshandeln fallen sensitive Daten zu Kritischen Infrastrukturen an, deren Schutz eine hohe Priorität genießen muss. Hier sollte gesetzlich klar geregelt werden, welche Daten von wem erhoben werden und an wen diese unter welchen Umständen weiterzugeben sind, um den Adressatenkreis solcher Daten klar abzugrenzen und somit den bestmöglichen Schutz dieser Daten zu gewährleisten.

Meldungen:
Das BSI hat bereits langjährige Erfahrung in der Entgegennahme, Auswertung und Bearbeitung von Meldungen über Störungen bei Kritischen Infrastrukturen gesammelt. In diesen Jahren haben sich die folgenden Punkte als zentral herausgestellt:

- Es sollte nur eine zentrale Meldestelle geben, um den KRITIS-Betreibern die Abgabe einer Störungsmeldung so einfach wie möglich zu machen. Das Letzte, was von einer wesentlichen Störung betroffene KRITIS-Betreiber brauchen, ist ein Wust von Meldepflichten, an verschiedene Behörden über verschiedene Meldeformulare. Da das BSI als zentrale Meldestelle etabliert ist und sich in dieser Funktion bewährt hat, muss diese zentrale Meldestelle beim BSI angesiedelt werden. Die Weiterleitung an andere Behörden, soweit dies notwendig und rechtlich vorgegeben ist, ist dann Angelegenheit der Umsetzung in den Behörden.
- Eine Formulierung von Meldeschwellen auf gesetzlicher Ebene ist aufgrund der sich stetig ändernden Bedrohungslage nicht möglich. Es ist daher wichtig, dass die umsetzenden Behörden Möglichkeiten bekommen, die Meldeschwellen und Kriterien anzupassen, so dass sichergestellt werden kann, dass weder zu viele Meldungen über unwichtige Ereignisse abgegeben werden müssen, was die Wirtschaft und das BSI belasten würde, ohne einen tatsächlichen Mehrwert zu erzeugen, noch besonders relevante Ereignisse nicht meldepflichtig sind, obwohl ihre Kenntnis und Analyse einen großen Beitrag zur Resilienz Kritischer Infrastrukturen leisten würde.

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?**

Antwort BSI: Dem BSI liegen hierzu keine Informationen vor.

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?**

Antwort BSI: Dies ist eine politische Frage (s. Bezug zu § 9b BSIG) und kann durch das BSI nicht beantwortet werden.

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?**

Antwort BSI: Die größte Herausforderung stellt der seit einigen Jahren spürbare Fachkräftemangel im technischen Bereich dar. Hier ist ein deutlicher Wettbewerb zwischen Arbeitgebern aus Wirtschaft und Verwaltung zu beobachten. Es gibt insgesamt mehr freie Stellen, als wir deutschlandweit Bewerbende haben. Dadurch können die Bewerbenden sich die Stellen aussuchen. Vor allem für Menschen, die ortsungebunden sind, sind das tolle Perspektiven. Insgesamt ist es schwieriger Stellen des gehobenen Dienstes zu besetzen, da viele Studierende nach dem Bachelor Abschluss auch einen Masterstudiengang anstreben.

Für staatliche (Sicherheits-)Behörden ist es wichtig, sich als attraktiver Arbeitgeber (Herausstellung der Benefits, Karrierewege, sicherer Arbeitsplatz, Vereinbarkeit von Familie, flexible Arbeitszeiten, Home-Office-Angebote, Einblicke in den Arbeitstag etc.) über eine eigene ansprechende Karriereseite, Arbeitgeberbewertungsplattformen sowie auf Karriere- und Fachveranstaltungen zu präsentieren.

Einen weiteren wichtigen Baustein bilden Aktivitäten im Personalmarketing, bei dem u.a. ein Fokus auf Hochschul-Kooperationen, Aktivitäten im Bereich Social Media und Businessnetzwerken gesetzt wird. Vor allem Karrieremessen, Exkursionen oder Vorträge an Hochschulen dienen dazu, potenzielle Bewerbergruppen zu interessieren. Das Angebot von Praktika und Abschlussarbeiten stellt zudem ein wichtiges Instrument der frühzeitigen Personalgewinnung dar.

Darüber hinaus ist es wichtig, sich mit der Zielgruppe zu beschäftigen: wer wird gesucht, wie möchte diese Zielgruppe angesprochen werden, was ist ihr wichtig, wo hält sich diese auf? Um dann über eine zielgruppenspezifische Ansprache in Stellenausschreibungen auf zielgruppenspezifischen Kanälen (von Jobbörsen bis hin zu Social Media) präsent zu sein.

Die „Candidate Experience“, also das Erlebnis von Jobinteressierten, über den Status als Bewerber/in hin zur/zum Mitarbeiter/in, ist positiv zu gestalten - im Sinne von einfach, schnell und digital. Ein möglichst vollständig digitalisierter Bewerbungsprozess ist für die Bewerbenden wie auch für die Recruiter/innen wichtig, um effektiver und effizienter arbeiten zu können. In der Bewerbendenkommunikation ist ein wertschätzender und verlässlicher Umgang entscheidend. Bewerbenden ist es wichtig, transparent über den Bewerbungsprozess mitgenommen zu werden, ebenso wie eine zeitnahe Zu- oder Absage.

Auswahlverfahren können – neben klassischen persönlichen Assessment Center – zunehmend per Videokonferenz angeboten werden. Bei den Bewerbenden kommen die Flexibilität und die moderne Ansprache gut an.

Zur Deckung der Bedarfe können Dauerausschreibungen eine Plattform für Initiativbewerbungen sein, um auch diejenigen anzusprechen, die auf der Karriereseite keine direkt passende Stelle finden. Die Möglichkeiten des Instrumentenkoffers, z.B. eine IT-Zulage, sind ebenfalls dienlich zur bestmöglichen Positionierung im Wettbewerb um die besten Köpfe.

Proaktiver geht es beim Active-Sourcing – dem gezielten Suchen nach geeigneten Kandidat/innen, die dann direkt mit einem Stellenangebot angesprochen werden. Ein Recruiting-Baustein, der gerade im öffentlichen Sektor – auch aufgrund der strengen Regularien – aktuell noch eher wenig Beachtung findet. Dadurch wird jedoch ein effektiver Recruiting-Kanal gegenwertig nicht ausgeschöpft.

Das Öffnen von Stellenausschreibungen für Abschlüsse ohne IT-Bezug, bei dem jedoch Bewerbende mit Berufserfahrung im IT-Bereich punkten können, stellt eine weitere Möglichkeit dar, dem aktuellen Fachkräftemangel sinnvoll zu begegnen.

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

Antwort BSI: Nach Ansicht des BSI kann die qualitativ/quantitative Ausbildung von IT-Cyberkräften insbesondere durch die Erweiterung von entsprechenden Schul-/Ausbildungs- und Studieninhalten branchenübergreifend bzw. integriert erreicht werden. Als Schlüsselkompetenz sollte sie bereits möglichst früh aufgebaut und lebenslang verstetigt werden. Insbesondere unter Berücksichtigung der hohen branchenübergreifenden Relevanz und gleichzeitig kurzer Halbwertszeit von IT-Wissen. IT-Sicherheit sollte auch in der Aus- und Weiterbildung integriert (mit-)gedacht werden, entsprechend eines ‚security by design' Ansatzes. Der Sinn und Zweck (der „Purpose", der für nachfolgende Generationen am Arbeitsmarkt entscheidend ist) ist damit klarer und macht das Thema möglicherweise auch als Berufsfeld interessanter. Darüber hinaus unterstützen konkrete Job- und Kompetenzprofile die berufliche Orientierung, die Personalgewinnung sowie die Qualifizierung von Cyber-Fachkräften. In Summe braucht es aber auch für die Qualifizierung gut geschultes und didaktisch kompetentes Lehrpersonal/Dozierende. Dies stellt eine weitere Herausforderung dar.

Bezüglich des Öffentlichen Dienstes: Auch eine stärkere Durchlässigkeit von Berufsabschlüssen im Öffentlichen Dienst, um im Vergleich zur Wirtschaft am derzeitigen Arbeitnehmermarkt konkurrenzfähig zu sein, wäre wünschenswert. Weitere Quereinsteiger-Programme zur Weiterqualifizierung könnten interessant sein. Im Sinne des Ansatzes vom lebenslangen Lernen braucht es weitere infrastrukturelle Rahmenbedingungen, wie z.B. virtuelle Qualifizierungsangebote, sowie die entsprechende Zeit zum Lernen im beruflichen Alltag.

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

Antwort BSI: Wie bereits in der Antwort auf Frage 3 dargestellt, können aktive Maßnahmen der Cyber-Abwehr in bestimmten Fällen eine sinnvolle Ergänzung der klassischen defensiven Cyber-Sicherheitsmaßnahmen sein. Das BSI verfügt über zahlreiche hochwertige Fähigkeiten bei der Erkennung, Analyse, Abwehr und Bewältigung von Cyber-Angriffen, die im Rahmen der rechtlichen Befugnisse beispielsweise beim Schutz der Regierungsnetze zum Einsatz kommen. Um diese weiter zu stärken, muss das BSI weiter als Sonderordnungsbehörde ausgebaut werden. Zu beachten ist allerdings, dass das Cyber-Sicherheitsniveau nicht nur durch staatliche Fähigkeiten und Befugnisse bestimmt wird, sondern vor allem auch durch die Umsetzung von Cyber-Sicherheitsmaßnahmen bei den Anwendern. Durch die fortgeschrittenen technischen Fähigkeiten der Angreifer, auch bei finanziell motivierten Angriffen, und das erfolgreiche Geschäftsmodell „Ransomware" der Täter ist Cyber-Sicherheit für Unternehmen und andere Einrichtungen eine teure und technisch-organisatorisch komplexe Aufgabenstellung geworden. Aufgrund der erheblichen Fixkosten, die für eine wirksame Cyber-Sicherheit aufgebracht werden müssen, sind kleine und mittelständische Einrichtungen hiervon besonders stark betroffen. Verschärft werden diese

Herausforderungen durch den Fachkräftemangel auf diesem Gebiet. Cybersicherheit muss „Chefinnensache“ bzw. „Chefsache“ in jedem Unternehmen sein. Bestehende Vorgaben und Empfehlungen im Bereich der Informations- und Cybersicherheit müssen konsequent umgesetzt werden.

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

Antwort BSI: Private Cyber-Sicherheitsunternehmen sind für das BSI wichtige Partner in unterschiedliche Bereichen. Um bestimmte Dienstleistungen skalierbar und auf hohem Niveau bereitstellen zu können, hat das BSI entsprechende Zertifizierungsverfahren für IT-Sicherheitsdienstleister und /oder Personen etabliert. Beispiele hierfür sind die Zertifizierungsverfahren für Dienstleister in den Bereichen Beratung, Revision und Penetrationstests.

Eine weitere wichtige Rolle privater Cyber-Sicherheitsunternehmen sind die Hersteller von Cyber-Sicherheitsprodukten. Um Ihre Informationsverarbeitung zu schützen, sind Anwender auf wirksame und praxistaugliche Cyber-Sicherheitsprodukte angewiesen. Hersteller können einerseits auf die vom BSI herausgegebenen Informationen zurückgreifen, um ihre Produkte zu optimieren, und andererseits bietet das BSI auch für Hersteller von Cyber-Sicherheitsprodukten geeignete Zertifizierungsverfahren an.

Wichtig für die Cyber-Sicherheit sind außerdem die Forschungsbeiträge privater Cyber-Sicherheitsunternehmen. Erkenntnisse über neuartige Angriffsmethoden, Schwachstellen und Schutzmechanismen fließen regelmäßig in die Verbesserung von Verfahren und Produkten ein, und somit auch in die Arbeit des BSI.

Des Weiteren könnte der vom BSI verfolgte Ansatz eines Cyber-Sicherheitsnetzwerkes durch ein konzertiertes Vorgehen die Cyber-Abwehr stärken.

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?

Antwort BSI: Siehe Antworten auf Fragen 4 und 7.

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?**

Antwort BSI: Für notwendige Grundsatzentscheidungen hinsichtlich eines Schwachstellenmanagements siehe die Antworten auf Frage 7. Darauf aufbauend ließen sich dann die technischen, personellen und organisatorischen Voraussetzungen eines staatlichen Umgangs mit Schwachstellen herausarbeiten.

Schon heute werden dem BSI bekannt gewordene Sicherheitslücken regelmäßig anhand von technisch-wissenschaftlichen Risikofaktoren und weiteren Erkenntnissen analysiert, um darauf aufbauend angemessen reagieren zu können (z.B. Warnen). Die unabhängigere Aufstellung stellt in diesem Kontext sicher, dass das BSI seine Aufgaben allein auf Grundlage wissenschaftlich-technischer Erkenntnisse wahrnimmt. Allerdings gehen die Vorteile einer unabhängigeren Aufstellung weit über die Frage des staatlichen Umgangs mit Schwachstellen hinaus (siehe Fragen 1, 2).

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?**

Antwort BSI: Das BSI versteht den souveränen Umgang von Nutzerinnen und Nutzern mit Informationstechnik als ganzheitliche Aufgabe, die es mit der Zielsetzung des Digitalen Verbraucherschutzes zu lösen gilt. Dafür

- schafft das BSI die Grundlagen und Rahmenbedingungen für Anbieter und Hersteller, um sichere und vertrauenswürdige Produkte und Dienste zu gestalten.
- informiert, berät und warnt das BSI die Verbraucherinnen und Verbraucher, damit sie digitale Produkte und Dienste sicher nutzen können.
- unterstützt das BSI die Verbraucherinnen und Verbraucher bei der Steigerung ihrer Resilienz, damit sie IT-Sicherheitsvorfälle bewältigen können.

Dieser Herausforderung begegnet das BSI mit einem umfassenden Portfolio unterschiedlich skalierter und auf verschiedenste Bevölkerungsgruppen sowie Bedürfnisse abgestimmter Maßnahmen. Zu diesen gehören unter anderem etliche medienübergreifende Sensibilisierungspublikationen, wie etwa Checklisten oder Broschüren (online und in Print verfügbar), zahlreiche Vorträge vor Verbraucherinnen und Verbrauchern und Fachpublikum, dynamische Formate bei Youtube und Instagram, Veranstaltungen wie die Gamescom, der Podcast ‚Update verfügbar', beständiger Austausch mit der Zivilgesellschaft über Formate wie den „Dialog für Cybersicherheit", regelmäßige Untersuchungen zur „IT-Sicherheit auf dem digitalen Verbrauchermarkt", gemeinsame Aktivitäten mit Kooperationspartnern,

Unternehmensdialog und Förderung von Unternehmensverantwortung, Aktivitäten der Standardisierung und Regelsetzung, das IT-Sicherheitskennzeichen, sowie die bundesweite Informations- und Sensibilisierungskampagne „#einfach aBSIchern“ gemeinsam mit dem BMI. Diese Produkte und Maßnahmen werden fortwährend evaluiert und auf die sich stets verändernden Rahmenbedingungen zugeschnitten. Ein Instrument hierfür ist das jährlich gemeinsam mit der Polizeilichen Kriminalprävention erhobene Digitalbarometer, eine Bürgerbefragung zu Einstellungen, Erfahrungen, Kenntnissen und Wünschen der Teilnehmenden rund um das Thema Cyber-Sicherheit.

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?

Antwort BSI: IT-Sicherheit ist eine gesamtgesellschaftliche Aufgabe. Ein hohes IT-Sicherheitsniveau kann nur erreicht werden, wenn alle digital agierenden Personen und Organisationen in Staat, Wirtschaft und Gesellschaft ein Mindestmaß an Schutzmaßnahmen, Aufmerksamkeit und Verhaltensregeln berücksichtigen. Dort, wo Informationen und Marktmechanismen nicht ausreichen, ist es Aufgabe des Staates, mit präventiven Angeboten und Regelungen steuernd zu gestalten. Gleichzeitig greift die staatliche Schutzpflicht zur Erkennung und Reaktion auf schwerwiegende Cyberangriffe auf seine eigenen Institutionen, Kritische Infrastrukturen, Unternehmen und Bürgerinnen und Bürger. Dieser Aufgabenbereich muss sich in den staatlichen Zuständigkeiten und Instrumenten zur Verbesserung der IT-Sicherheit widerspiegeln. Das BSI als die nationale Cyber-Sicherheitsbehörde nimmt dabei auf der Grundlage seiner integrierten Wertschöpfungskette der Cybersicherheit (Prävention, Detektion, Reaktion für Staat, Wirtschaft und Gesellschaft) eine besondere Rolle ein. Die Vorhaben des Koalitionsvertrags zur Stärkung der IT-Sicherheit und des BSI sind hiesigen Erachtens richtige und wichtige Schritte, um die staatliche Handlungsfähigkeit für die Sicherheit in der Digitalisierung langfristig zu gewährleisten. Ein ganz wesentlicher Erfolgsfaktor für die Handlungsfähigkeit ist dabei der Ausbau von Ausbildungs- und Weiterbildungsmöglichkeiten sowie die Förderung und staatliche Anstellung von IT-Sicherheitsexpertinnen und -experten.

Weitere konkrete Verbesserungsmöglichkeiten zur Erhöhung der IT-Sicherheit können aus BSI-Sicht sein: Aus Sicht des BSI ist es essentiell, dass das BSI frühzeitig in entsprechenden Überlegungen bzw. Projekten eingebunden wird. Nur so kann präventiv IT-Sicherheit bereits in der Konzeption berücksichtigt werden. Dabei sollte das BSI als zentraler IT-Sicherheitsdienstleister des Bundes eine entsprechend starke zentrale Position mit den notwendigen Ressourcen in der Bundesverwaltung haben.

Mögliche (technische) Instrumente sind (Auswahl):

- Geeignete durch BSI erstellte bzw. bestätigte Technische Vorgaben und Prüfspezifikationen,
- Konzeption/Bewertung/Bereitstellung von Sicherheitsinfrastrukturen (PKI, eID, NPKD),
- Verwendung von Zero Trust Architekturen,
- starke Sicherheitsanker (HW, aktuelle Krypto, TEE, TSP),
- Risikomanagement,
- sichere Anwendungen/Apps – sowohl Produkte als auch Hintergrundsysteme (Server, Cloud), wie zum Beispiel Corona-Warn-App (CWA), AusweisApp2 (AA2), Automotive,
- BSI-eigene Analyseinfrastrukturen ermöglichen eigene Penetrationstests und funktionale Wirksamkeitsanalysen,
- Schwachstellenmonitoring und zielgruppenorientierte Kommunikation,
- Sicherheitsinformationen müssen Endnutzer erreichen (hierzu gegebenenfalls Ausbau des IT-Sicherheitskennzeichens),
- Monitoring der Behebung von Schwachstellen,
- Verpflichtung zu Updates (siehe auch den aktuellen EU-Vorschlag zum Cyber Resilience Act (CRA)),
- Sicherheitslösungen und PoC,
- sichere Kommunikationsinfrastrukturen und sichere, vertrauenswürdige Provider.

Security by Design:
Die Sicherheitseigenschaften von (digitalen) Produkten/Diensten sind nicht transparent für den Nutzenden, da es keine Informationspflichten seitens des Herstellers gibt. Im Zuge immer kürzerer Entwicklungszyklen in Verbindung mit dem Wunsch nach neuen Funktionen, kann Cyber-Sicherheit im Entwicklungsprozess nur wenig Berücksichtigung finden. Sichere Entwicklungsprozesse im Sinne eines darauf angepassten Qualitätsmanagementsystems sind Zeit- und Kostenintensiv, u.a. aufgrund von Dokumentationspflichten und den damit verbundenen fachlich qualifizierten Mitarbeitenden. Stattdessen ist es üblich auf eine Vielzahl an Fremdkomponenten von Drittherstellern bzw. Open Source zuzugreifen, die wiederum weitere Komponenten benötigen, sodass der Hersteller des Endproduktes selbst kaum einen Überblick über die verwendeten Komponenten und deren Schwachstellen hat. Durch sichere Entwicklungsprozesse in Verbindung mit den Möglichkeiten der Erstellung und Pflege einer Software-Stückliste („Software Bill of Materials“) und maschinenlesbaren Schwachstellenbeschreibungen könnten viele dieser Probleme durch Automatisierung mitigiert werden. Durch eine Informationspflicht zu Sicherheitseigenschaften, kann eine Bewertung der Cyber-Sicherheit von Produkten/Diensten, z.B. anhand der „Software Bill of Materials“ in Bezug auf den spezifischen Einsatz erfolgen.

Cyber-Crime:
Vor dem Hintergrund des anhaltenden Erfolgs des Geschäftsmodells „Ransomware“ der Angreifer im Bereich Cyber-Crime sollte aus Sicht des BSI geprüft werden, ob Verbesserungen der Cyber-Sicherheit durch Eingriffe in die Finanzierung der Tätergruppen flankiert werden sollten. Hierzu sollten insbesondere folgende Aspekte betrachtet werden:

- Sollten Löse-, Schweige- und Schutzgeldzahlungen von Betroffenen im Zuge von Cyber-Angriffen – zumindest in bestimmten Fällen – untersagt werden?
- Sollte die Versicherbarkeit von Löse-, Schweige- und Schutzgeldzahlungen bei Cyber-Angriffen eingeschränkt werden?
- Welche anderen Instrumente gibt es, um die Finanzierung der Cyber-Angreifer zu erschweren?

Siehe auch die Antworten auf Frage 13 zur grundsätzlichen Herausforderung der Anwender und auf Frage 1 zur Rolle des Cyber-Abwehrzentrums.

Bildung:
In Bezug auf die Verbesserung im Bereich Bildung müssen in erster Linie alle Bildungspartner von Schulen, über Verantwortliche für Ausbildung und Studium bis zum Weiterbildungssektor in den Fokus genommen werden. Ein frühzeitiges „in Kontakt kommen“ ist relevant für das Interesse und somit auch den Erfolg. Insofern kommt Schulen und weiterentwickelten Lehrplänen eine wichtige Funktion zu. Nach wie vor gibt es bei Schulen und Lehrpersonal meist nur wenige Berührungspunkte mit dem Thema IT-Sicherheit. Ferner sollte Cyber-Sicherheit Pflichtmodul in sämtlichen IT-Studiengängen sein. So sollte z.B. sicheres Programmieren fester Bestandteil der Studienordnung sein.

Die Bundesagentur für Arbeit könnte auch eine zentrale arbeitsmarktpolitische Rolle bezüglich Jobprofilen und entsprechenden Kampagnen zur Steigerung der Aufmerksamkeit für das Thema spielen.

***