Deutscher Bundestag **Drucksache 20/8707**

20. Wahlperiode 09.10.2023

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/8103 –

Digitale Souveränität in der Bundesverwaltung – Entwicklung, Beschaffung und Einsatz von IT-Sicherheitsprodukten

Vorbemerkung der Fragesteller

Die Bundesverwaltung ist vom einwandfreien Funktionieren und der uneingeschränkten Verfügbarkeit von IT-Systemen abhängig (www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/IT-Sicherheiskriterien/it-sicherheiskriterien_node.html; www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Grundsaetzliche-Aussagen/grundsaetzliche-aussagen_node.html).

Deshalb hat unter anderem das Bundesamt für Sicherheit in der Informationstechnik (BSI) einerseits nach dem BSI-Gesetz (BSIG) und der BSI-Zertifizierungs- und Anerkennungsverordnung die Aufgabe, Zertifizierungen informationstechnischer Produkte oder Komponenten sowie informationstechnischer Systeme durchzuführen. Zertifikate des BSI sind ein unabhängiger Konformitätsnachweis dahin gehend, dass ein IT-Sicherheitsprodukt definierten Sicherheitsanforderungen entspricht. In einigen Bereichen ist eine Zertifizierung durch Gesetz, Verordnung, Richtlinie oder Standard verbindlich vorgeschrieben. Für die Produktzertifizierung empfiehlt das BSI eine Zertifizierung nach den international anerkannten Sicherheitskriterien der Common Criteria (CC). Die CC sind ein etablierter und international anerkannter Kriterienkatalog für das Design, die Implementierung, Auslieferung und Wartung der Sicherheitsfunktionen von IT-Sicherheitsprodukten. Für die Zertifizierung nach den CC wurde international die gegenseitige Anerkennung von IT-Sicherheitszertifikaten unter gewissen Bedingungen vereinbart, um die Mehrfach-Zertifizierung des gleichen Produkts in verschiedenen Staaten zu vermeiden. Mit einem CC-Zertifikat bestätigt das BSI die Korrektheit und Effektivität der vom Produkt angebotenen Sicherheitsfunktionen. Eine Zertifizierung kann auch nach einer Technischen Richtlinie (TR) erfolgen. Ein wesentlicher Bestandteil davon ist die Konformitätsprüfung, in der untersucht wird, ob ein Produkt die in der jeweiligen TR festgelegten Vorgaben und Anforderungen erfüllt. Das Ziel einer TR des BSI ist die Verbreitung von angemessenen IT-Sicherheitsstandards. Ihre Verbindlichkeit entsteht erst durch individuelle Vorgabe des Bedarfsträgers. Die europäisch anerkannten ITSEC-Sicherheitskriterien (ITSEC = Information Technology Security Evaluation Criteria) können einerseits für eine Produktzertifizierung im BSI-Zertifizierungsschema nur noch in begründeten

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 4. Oktober 2023 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Ausnahmefällen angewandt werden (www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/zertifizierung-und-anerkennung_node.html; www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/zertifizierung-nach-cc_node.html; www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/itsicherheitszert.html?nn=127290; www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/CC-Produkte.pdf?__blob=publicationFile&v=10; Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen (bund.de); www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Zertifizierte-IT-Sicherheit.pdf?__blob=publicationFile&v=1).

Andererseits hat das BSI auch die vertrauensbildende gesetzliche Aufgabe, IT-Produkte für die Sicherheit in der IT zu prüfen und eine verbindliche Aussage zum Sicherheitswert zu machen. Betroffen sind IT-Produkte, die zudem für die Übertragung und Verarbeitung von amtlich geheim gehaltenen Informationen im Geheimschutz und in Verschlusssachen (VS) im Bereich des Bundes und der Länder oder bei Unternehmen im Rahmen von Aufträgen des Bundes oder der Länder eingesetzt werden. Derartige Produkte benötigen eine Zulassung durch das BSI. Das BSI legt überdies fest, welche IT-Sicherheitsprodukte über eine Zulassung verfügen müssen. Diese IT-Sicherheitsprodukte im Bereich der Informationstechnik zur Handhabung von Verschlusssachen einschließlich deren Übertragung (VS-IT) übernehmen IT-Sicherheitsfunktionen zum Schutz elektronischer VS. Der Antrag auf Zulassung eines solchen IT-Produkts kann grundsätzlich nur von einem behördlichen Anwender gestellt werden. Sind keine zugelassenen IT-Sicherheitsprodukte für VS-IT vorhanden oder kann eine Bereitstellung nicht zeitgerecht veranlasst werden, kann beim BSI eine Einsatzerlaubnis für andere IT-Sicherheitsprodukte beantragt werden. Das BSI kann diese Einsatzerlaubnis zeitlich befristen sowie besondere Auflagen und Einschränkungen hinsichtlich der Einsatz- und Betriebsbedingungen erteilen. Von der Zulassungsregelung sind begrenzt auch solche IT-Sicherheitsprodukte betroffen, die für sensitive, aber nicht eingestufte Informationen im Behördenbereich eingesetzt werden können. Grundsätzlich gilt eine solche Zulassungsregelung für den Bereich der sensitiven, aber nicht eingestuften Informationen aber nicht (Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz [Verschlusssachenanweisung – VSA] vom 13. März 2023, § 5 Absatz 1 Nummer 5 und 6 sowie § 51 Absatz 1 und 5 VSA; www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/Hinweise-zur-Liste-der-zugelassenen-IT-Sicherheitsprodukte-und-systeme/hinweise-zur-liste-der-zugelassenen-it-sicherheitsprodukte-und-systeme.html; www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/FAQ-Zertifizierung-und-Anerkennung/faq-zertifizierung-und-anerkennung_node.html).

Zudem unterscheidet das BSI in IT-Sicherheitsprodukte, die vom BSI zugelassen sein müssen, und IT-Sicherheitsprodukte, die zugelassen sein sollen. Letztere lassen Ausnahmen zu, falls keine geeigneten zugelassenen Produkte zur Verfügung stehen. In der Regel kommen dabei IT-Sicherheitsprodukte zum Einsatz, die durch das BSI mit nationalem Schutzprofil CC-zertifiziert wurden (www.bsi.bund.de/DE/Service-Navi/FAQ/EvaluierungundZulassung/faq_evaluierung-zulassung_node.html).

Die VSA listet zudem IT-Sicherheitsfunktionen innerhalb von VS-IT, die Gegenstand einer Zulassungsaussage des BSI sein können. Das BSI hat einen auf diesen IT-Sicherheitsfunktionen und den sich hieraus ableitenden Produktklassen und Produkttypen basierenden Katalog veröffentlicht (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zulassung/VS-Produktkatalog_BSI.pdf?__blob=publicationFile&v=13). Der Katalog der Produktklassen und Produkttypen definiert insbesondere, ob eine Zulassungsaussage für einen Produkttyp erforderlich ist und welche Sicherheitsfunktionen in einem Zulassungsverfahren für einzelne Produkttypen gelten (§ 52 VSA).

Im Übrigen unterstützen und beraten die IT-Sicherheitsbeauftragten die Geheimschutzbeauftragten in der Verwaltung in allen Fragen des Einsatzes von VS-IT (§ 9 VSA).

Neben den IT-Sicherheitsprodukten für VS-IT darf aber nicht unerwähnt bleiben, dass selbstverständlich auch solche IT-Sicherheitsprodukte, die nicht im Bereich der Verschlusssachen eingesetzt werden, Relevanz für die ganzheitliche digitale Souveränität der Bundesverwaltung haben. Denn häufig bekommen Dienstleister auch mit diesen IT-Sicherheitsprodukten Einblicke in den Daten- und Netzverkehr. Dies kann z. B. bei Schutzlösungen für die sogenannten Layer 3, 4 und 7 oder den E-Mail-Verkehr der Fall sein. Diese IT-Sicherheitsprodukte sind daher auch von Interesse für die Fragesteller in der vorliegenden Kleinen Anfrage.

Darüber hinaus existieren in der Wirtschaft Einrichtungen, deren Beeinträchtigung Gefahren für das Leben oder die Gesundheit der Bevölkerung, für die öffentliche Sicherheit oder Ordnung sowie die Verteidigungsbereitschaft des Landes hervorrufen können. Eine besondere Gefahr kann dabei immer von Personen ausgehen, die in diesen Einrichtungen tätig sind. Durch die Geheimschutzbetreuung der Firmen beispielsweise in Form von Sicherheitsüberprüfungen der VS-befassten Mitarbeiterinnen und Mitarbeiter, und durch den vorbeugenden Sabotageschutz, etwa in Form von Sicherheitsüberprüfungen von Mitarbeitern, die an sicherheitsempfindlichen Stellen eingesetzt werden sollen, begegnen die zuständigen Geschäftsbereiche der Bundesregierung basierend auf den gesetzlichen Regelungen des Sicherheitsüberprüfungsgesetzes (SÜG) diesen Gefahren (www.bmwk.de/Redaktion/DE/Artikel/Wirtschaft/sicherheit-in-der-wirtschaft.html).

In der Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat (BMI) vom Juli 2022 wird betont, dass die Stärkung der Cyber-Resilienz von Bundesbehörden keinen weiteren Aufschub duldet. Unter anderem fordert es, dass Bundesbehörden mit weiterentwickelten IT-Produkten ausgestattet werden sollen (www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4, S. 5, S. 10.). In ihrer Digitalstrategie erhebt die Bundesregierung zudem den Anspruch, die Erforschung, Anwendung und Einführung von Schlüsseltechnologien als Grundlage für digitale Souveränität konsequent voranzutreiben. In diesem Zusammenhang beabsichtigt die Bundesregierung, unter anderem die Kompetenzen in der Cybersicherheit auszubauen und ganzheitlich das dazugehörende Ökosystem zu stärken (Digitalstrategie, S. 33 f., abrufbar unter: digitalstrategie-deutschland.de/static/fcf23bbf9736d543d02b79ccad34b729/Digitalstrategie_Aktualisierung_25.04.2023.pdf). Darüber hinaus vertritt die Bundesregierung in ihrer kürzlich veröffentlichten Nationalen Sicherheitsstrategie den Anspruch, im Zusammenhang mit einer Weiterentwicklung der Cybersicherheitsstrategie auch die Cybersicherheit der Bundesverwaltung umfassend zu stärken (Nationale Sicherheitsstrategie der Bundesregierung, Bundestagsdrucksache 20/7220, S. 59, S. 61). Auch adressiert sie in der Nationalen Sicherheitsstrategie wichtige Fragen zur Beschaffung von Sicherheitstechnologien als Schlüssel-technologien an prominenter Stelle. So heißt es unter anderem, dass es „[…] eines gezielten Auswahlprozesses, der Wissensentwicklung und -verbreitung, der Rahmensetzung, der Ressourcenmobilisierung und Marktentwicklung für strategische Technologielinien [bedürfe]“ (Nationale Sicherheitsstrategie der Bundesregierung, Bundestagsdrucksache 20/7220, S. 57) und die Bundesregierung werde „[…] überprüfen, bei welchen Schlüsseltechnologien nationale und europäische Fähigkeiten zum Schutz unserer technologischen und digitalen Souveränität nötig sind [und] gezielt Anbieter kritischer Schlüsseltechnologien mit geeigneten Maßnahmen, z. B. durch staatliche Ankeraufträge, unterstützen, um eigene Fähigkeiten zu Forschung und Entwicklung in kritischen Technologien zu erhalten und weiterzuentwickeln“ (Nationale Sicherheitsstrategie der Bundesregierung, Bundestagsdrucksache 20/7220, S. 58).

Unter dem Eindruck der obigen Ausführungen rund um Zertifizierung, Zulassung und Sicherheitsüberprüfungen im gesamten Bereich von IT-Sicherheits-

produkten – also denen für den Einsatz im Bereich von VS-IT als auch denen für den Einsatz abseits von Verschlusssachen – und den dargestellten Ansprüchen der Bundesregierung in der Cybersicherheit und zur digitalen Souveränität ergeben sich für die Fraktion der CDU/CSU Fragen zur Beschaffung und zum Einsatz von IT-Sicherheitsprodukten für die Bundesverwaltung (Hinweis: Bei den folgenden Fragen mit Bezug zur Bundesverwaltung sind die Nachrichtendienste des Bundes auszunehmen.).

Vorbemerkung der Bundesregierung

Eine lückenlose Auflistung der in der Bundesverwaltung eingesetzten IT-Sicherheitsprodukte nach den angefragten Merkmalen, wie z. B. die jeweilige Anzahl der Installationen und die jeweilige Anzahl der Produktlizenzen, kann bei der Beantwortung der vorliegenden Kleinen Anfrage nicht gewährleistet werden. Die in der Bundesverwaltung eingesetzten IT-Sicherheitsprodukte werden nicht zentral erfasst; hierzu besteht auch keine Verpflichtung. Die Beantwortung der Frage erforderte daher eine umfangreiche Auswertung eines erheblichen dezentralen Informationsbestandes, welche die Ressourcen der zuständigen Stellen in der gesamten Bundesverwaltung in dem für die Beantwortung der Frage zur Verfügung stehenden Zeitraum in erheblichem Maße beanspruchte und sich auf deren Aufgabenerfüllung auswirkte. Die nachfolgenden Ausführungen bzw. aufgeführten Angaben erfolgen auf der Grundlage der vorliegenden Erkenntnisse sowie vorhandener Unterlagen und Aufzeichnungen. Diesbezügliche Daten sind somit möglicherweise nicht vollständig.

Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich öffentlich, transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit erfragte Informationen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann und gegebenenfalls alternative Formen der Informationsvermittlung zu suchen, die das Informationsinteresse des Parlaments unter Wahrung der berechtigen Geheimhaltungsinteressen der Regierung befriedigen (BVerfGE 124, 161,193).

Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass die erstellte Zusammenstellung zur Beantwortung der Fragen 11 und 14 bis 17 nicht offen erfolgen kann und eine Einstufung der Zusammenstellung als „VS – Nur für den Dienstgebrauch“ gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) notwendig macht.* Die IT-Infrastruktur der Bundesregierung ist jeden Tag einer Vielzahl unterschiedlicher Angriffe ausgesetzt. Zur Aufrechterhaltung der Staats- und Regierungsfunktion ist diese Infrastruktur angemessen zu schützen. Eine Beeinträchtigung oder sogar Ausfall auf Grund erfolgreicher Cyberangriffe muss bestmöglich verhindert werden.

Die Beantwortung und detaillierte Auflistung von sämtlichen in der Bundesverwaltung eingesetzten IT-Sicherheitsprodukten ermöglicht es etwaigen Angreifern, konkrete Hinweise zu den in der Bundesverwaltung eingesetzten Schutzmaßnahmen zu erhalten. Unter Kenntnis der durch die Bundesverwaltung ein-

* Das Bundesministerium des Innern und für Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

gesetzten Produkte können Angreifer produktspezifische Schwachstellen ausmachen und diese gezielt ausnutzen.

Die darüber hinaus erfragte Zuordnung eingesetzter IT-Sicherheitsprodukte auf einzelne Ressorts oder Behörden würde es Angreifern deutlich einfacher machen, gezielt Sicherheitslücken auszunutzen und einzelne Ressorts oder Behörden gezielt anzugreifen. Die insoweit erbetenen Informationen zielen auf den Einsatz von IT-Sicherheitsprodukten in jeder einzelnen Bundesbehörde ab. Mit der Beantwortung würde offengelegt, wie sich einzelne Ressorts oder Behörden vor Cyberangriffen schützen, und potentiellen Angreifern würden wichtige Hinweise für etwaige Angriffe ermöglicht. Eine Aufschlüsselung nach Ressorts oder Behörden könnte ggf. zu Rückschlüssen über die Sicherheitserheblichkeit der dort jeweils verarbeiteten Daten führen und so Angriffsziele identifizieren. Eine ressort- oder behördenspezifische Aufschlüsselung zu eingesetzten IT-Sicherheitsprodukten würde gezielte elektronische Angriffe auf einzelne Behörden ermöglichen. Wird beispielsweise eine Sicherheitslücke bei einem der eingesetzten Produkte bekannt, könnten Angreifer dies gezielt und schnell ausnutzen, da bekannt ist, welche Behörde diese Produkte einsetzt. Dies gefährdet die Arbeitsfähigkeit und somit die Erfüllung des gesetzlichen Auftrags der betroffenen Behörden und gefährdet letztlich die Informationssicherheit der gesamten Bundesverwaltung erheblich.

Es muss deshalb potentiellen Angreifern verborgen bleiben, welche IT-Sicherheitsprodukte in welchen Behörden zum Schutz der IKT-Infrastrukturen und darin verarbeiteten Daten eingesetzt werden.

Eine Hinterlegung der angefragten Informationen hinsichtlich der die jeweiligen IT-Sicherheitsprodukte einsetzenden Behörde sowie des Geschäftsbereichs der vertragsschließenden Bundesbehörde in der Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung für die Aufgabenerfüllung der Bundesverwaltung nicht in Betracht. Das Risiko, dass derart sensible Informationen bekannt werden, kann unter keinen Umständen hingenommen werden. Die angefragten Informationen beschreiben die Sicherheitsmaßnahmen des Bundes aufgrund ihres Bezuges auf bestimmte Produkte bzw. Hersteller in einem derartigen Detaillierungsgrad, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen würde.

Würden potentielle Angreifer detaillierte Kenntnis über Verbreitung und Produktdetails der jeweiligen IT-Sicherheitsprodukte erhalten, wäre ein Angriff auf die jeweilige Behörde deutlich einfacher zu gestalten und mit höherer Erfolgsaussicht verbunden. Zum Beispiel würde die Kenntnis über der jeweiligen Firmware oder Softwarestand den Angreifer in die Lage versetzen, gezielt Zero-Day-Exploits der eingesetzten IT-Sicherheitsprodukte zu identifizieren oder zu erwerben und diese Schwachstelle auszunutzen. Da für Zero-Day-Exploits i. d. R. keine Gegenmaßnahmen wie z. B. Sicherheitsupdates des Herstellers möglich sind, wären die Behörden einem Angriff ungeschützt ausgesetzt.

Die Fragen 11 und 14 bis 17 können daher nur in einer Form beantwortet werden, die eine Zuordnung eingesetzter IT-Sicherheitsprodukte zu einzelnen Behörden nicht ermöglicht, und bereits diese Zusammenstellung muss aus den oben genannten Gründen als „VS – Nur für den Dienstgebrauch“ eingestuft werden.*

Auch hinsichtlich der Beantwortung der Frage 19 ist angesichts der vorstehend geschilderten Sicherheitsrisiken eine Einstufung als „VS – Nur für den Dienstgebrauch“ erforderlich. Sicherheitsrisiken bestehen, wenn durch das Bekannt-

* Das Bundesministerium des Innern und für Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

werden der Geheimschutzbetreuung in diesem Kontext die geheimschutzbetreuten Unternehmen Ziel von besonderen Gefährdungen, insbesondere durch ausländische Nachrichtendienste, werden können und damit die Gefahr der Kompromittierung von Verschlusssachen erhöht wird.*

1. In welchen Bereichen ist eine Zertifizierung von IT-Sicherheitsprodukten durch Gesetz, Verordnung, Richtlinie oder Standard verbindlich vorgeschrieben?

Die erbetenen Informationen können der nachstehenden Auflistung entnommen werden.

Bereiche, die eine (Common Criteria) CC-Zertifizierung aufgrund spezialgesetzlicher Regelungen fordern:

- Digitale Tachograph-Systeme (Vehicle Unit, Motionsensor, Chipkarten) – EU Regulierung: Durchführungsverordnung (EU) 2016/799 der Kommission vom 18. März 2016 zur Durchführung der Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates zur Festlegung der Vorschriften über Bauart, Prüfung, Einbau, Betrieb und Reparatur von Fahrtenschreibern und ihren Komponenten
- Hoheitliche Dokumente: Reisepass, Aufenthaltstitel, Personalausweis (PassG, PAuswG)
- Registrierkassen/Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme: Sicherheitsmodul und Teile der Anwendungssoftware (KassenSichV)
- Gesundheitswesen/eHealth: Gesundheitskarte (Chipkarten), Kartenterminal (mobil und stationär), Netzkonnektor (SGB V)
- Digitalisierung der Energiewende: Smart Meter Gateway inkl. Sicherheitsmodul (Messstellenbetriebsgesetz – MsbG)

Für (Technische Richtlinien) TR-Zertifizierung:

- De-Mail-Gesetz (De-Mail-G)
- Gesetz über Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG)
- Passgesetz (PassG)
- Verordnung zur Erfassung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke in den Passbehörden und der Übermittlung der Passantragsdaten an den Passhersteller (Passdatenerfassungs- und Übermittlungsverordnung – PassDEÜV)
- Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz –PAuswG)
- Verordnung über Personalausweise, eID-Karten für Unionsbürger und angehörige des Europäischen Wirtschaftsraums und den elektronischen Identitätsnachweis (Personalausweisverordnung – PAuswV)
- Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz – AufenthG)
- Aufenthaltsverordnung (AufenthV)

* Das Bundesministerium des Innern und für Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

- Asylgesetz (AsylG)
- Verordnung über die Bescheinigung über die Meldung als Asylsuchender (Ankunftsnachweisverordnung – AKNV)
- Sozialgesetzbuch Fünftes Buch (SGB V)
- Kassensicherungsverordnung (KassenSichV)

Für (Beschleunigte Sicherheitszertifizierung) BSZ & (Network Equipment Security Assurance Scheme) NESAS-Zertifizierung:

Telekommunikationsinfrastrukturen, 5G-Cybersicherheit (§ 165 Absatz 4 TKG)

Für deutsche hoheitliche Dokumente ist eine IT-Sicherheits-Zertifizierung aufgrund folgender Gesetze und Verordnungen vorgeschrieben:

- Reisepässe: EU-Verordnung (EG) Nr. 2252/2004, EU-Durchführungsbeschluss C(2018) 7774
- Personalausweise: EU-Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates, EU-Durchführungsbeschluss C(2018) 7767, PAuswG, PAuswV, BSI TR-03127
- Elektronische Aufenthaltstitel: EU-Verordnung (EG) Nr. 1030/2002 des Rates, EU-Durchführungsbeschluss C(2018) 7767
- Zudem müssen bestimmte Komponenten zur Antragsdatenerfassung für hoheitliche Dokumente aufgrund der PAuswV und der BSI TR-03127 zertifiziert sein.

Für IT-Produkte (nicht Infrastrukturen) und verbindlich (als eigenständige Zertifizierung, nicht Baustein/Komponente in einer anderen Zertifizierung):

- Verpflichtung zum Einsatz zertifizierter Technischer Sicherheitseinrichtungen zum Schutz von Aufzeichnungen elektronischer Aufzeichnungssysteme gemäß § 146a AO und KassenSichV
- Verpflichtung zum Einsatz zertifizierter Krypto-Module (HSMs/Chipkarten) für gewisse PKI-Teilnehmer (z. B. Sub-CAs und relevante Endnutzer der PKI) in der Berechtigungs-PKI für eID-Dokumente gemäß Certificate Policy der CVCA, welche durch § 32 PAuswV und VÖ im Bundesanzeiger verbindlich ist.

Im Mobilitätskontext machen für den Bereich C-ITS (Cooperative Intelligent Transport Systems) die „C-ITS Certificate Policy“ und die „C-ITS Security Policy“ verbindliche Vorgaben als Teilnahmevoraussetzungen zur europaweiten Public Key Infrastruktur (PKI) für C-ITS.

Für die Telematikinfrastruktur ist die Pflicht zur Sicherheitszertifizierung in § 325 Abs. 3 SGB V festgelegt.

Für den Bereich „Hoheitliche Biometrie“ besteht gegenwärtig Zertifizierungspflicht für Equipment und Systeme, die für die Erfassung und Verarbeitung von Biometrie verwendet werden:

- im deutschen Pass- und Ausweiswesen gem. PAuswG § 12 und PAuswV § 2 i. V. m. Anhang 4, PassDEÜV § 2 i. V. m. Anlage 1 und 2, sowie AufenthG § 49 und AufenthV § 76b
- im deutschen Ausländerwesen gem. AKNV § 1 i. V. m. Anlage 1
- Die Zertifizierung erfolgt nach der BSI TR-03121

Mit Bezug zu § 19 Gleichstellungswahlverordnung:

Sicherheitstechnische Anforderungen an Wahlprodukte sowie Mindestanforderungen an die Informationssicherheitskonzepte und die Notfallkonzepte in einer technischen Richtlinie für elektronische Wahlen.

2. Von welchem Zeitraum genau geht die Bundesregierung bei einer nicht „zeitgerechten“ Veranlassung von zugelassenen IT-Sicherheitsprodukten für VS-IT und einer daraus gegebenenfalls notwendig werdenden Beantragung einer Einsatzerlaubnis für andere IT-Sicherheitsprodukte als die zugelassenen IT-Sicherheitsprodukte für VS-IT aus?

Der Zeitraum wird individuell im Rahmen eines konkreten Zulassungsverfahrens unter Einbeziehung relevanter beteiligter Parteien (Antragsteller, Produkthersteller und BSI-Zulassungsschema) festgelegt. Begründet sein kann das Erfordernis einer Einsatzerlaubnis z. B. durch verzögerte Entwicklung des IT-Sicherheitsproduktes, Evaluierungserkenntnisse, die eine Produktanpassung erfordern oder eine begründete sehr kurzfristige Nutzungsnotwendigkeit des Bedarfsträgers. Über die Annahme eines Antrags auf Einsatzerlaubnis wird in den entsprechenden Gremien des BSI-Zulassungsschemas in gleicher Weise entschieden wie bei einem Antrag auf Zulassung.

3. Welche genauen Produkttypen von IT-Sicherheitsprodukten, die für sensitive, aber nicht eingestufte Informationen im Behördenbereich eingesetzt werden können, sind in welchen Bereichen begrenzt von der Zulassungsregelung betroffen?

Keine, da „Zulassung“ ein Begriff aus den Regelungen des Geheimschutzes/der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) ist und sich ausschließlich auf den Schutz von Verschlusssachen bezieht.

4. Welche Produkttypen von IT-Sicherheitsprodukten umfasst für welche Bereiche gemäß der Unterscheidung des BSI bei IT-Sicherheitsprodukten solche IT-Sicherheitsprodukte, die vom BSI zugelassen sein sollen, und um welche Ausnahmen genau handelt es sich, falls keine geeigneten zugelassenen Produkte zur Verfügung stehen?

Die Zulassungsrelevanz von IT-Sicherheitsprodukten und -komponenten wird gemäß § 52 VSA durch den vom BSI herausgegebenen Katalog von Produktklassen und -typen geregelt (VS-Produktkatalog). Darin legt das BSI abgestuft nach den Geheimhaltungsgraden gemäß § 4 VSA fest, ob für ein Produkt eines bestimmten Produkttypen eine Zulassung erforderlich ist. Beantragt werden kann eine Zulassung für ein IT-Sicherheitsprodukt durch einen bundesbehördlichen Bedarfsträger. Diesem Antrag muss ein entsprechender Bedarf zum Schutz von elektronischer VS mittels des beantragten Produktes zugrunde liegen. Wird der durch den Zulassungsantrag geäußerte Bedarf durch das Zulassungsschema des BSI anerkannt, kann aber nicht oder nicht zeitgerecht durch eine Zulassung gedeckt werden, so ist für diesen Ausnahmefall die Beantragung einer Einsatzerlaubnis möglich.

5. Ist das Amt des IT-Sicherheitsbeauftragten einer Bundesverwaltung oder einer Bundesbehörde bei der Auswahl eines zu beschaffenden IT-Sicherheitsprodukts beteiligt, und wenn ja, wie genau ist es daran beteiligt, und bei welchen Bundesverwaltungen und Bundesbehörden ist das regelmäßig der Fall (bitte auflisten)?

In der Bundesverwaltung gelten die Vorgaben der „Leitlinie für Informationssicherheit in der Bundesverwaltung“ (UP Bund). Darin ist die Umsetzung des Grundschutzes nach BSI-Standards (200-1 bis -3, in der Standardabsicherung) als Mindestanforderung festgelegt. Diese definieren auch die Aufgaben eines IT-Sicherheitsbeauftragten als Teil des einzurichtenden Informationssicherheitsmanagement (ISM) der Behörden. Der IT-Sicherheitsbeauftragte (bzw. das durch ihn gesteuerte ISM der Behörde) ist demnach in allen Bundesbehörden angemessen (und regelmäßig) an Beschaffungen von IT-Sicherheitsprodukten zu beteiligen. Die konkrete Art der Umsetzung obliegt der jeweiligen Behörde (bzw. dem zuständigen Ressort) und kann daher im Detail aufgrund unterschiedlicher Anforderungen oder Besonderheiten in der Organisation unterschiedlich gelöst sein. Der IT-Sicherheitsbeauftragte kann in Behörden z. B. selber für Beschaffung (und Auswahl) von IT-Sicherheitsprodukten verantwortlich sein oder er ist im Rahmen der Planung, des Anforderungsmanagements oder Beschaffungsprozesses der Behörde geeignet eingebunden. In diesen Fällen kann er z. B. Anforderungen an die Informationssicherheit definieren oder es muss vor Beschaffung zumindest seine Mitzeichnung eingeholt werden.

6. Plant die Bundesregierung, für den vom Bundesinnenministerium in seiner Cybersicherheitsagenda vorgeschlagenen CISO Bund (CISO = Chief Information Security Officer) Kompetenzen (siehe Cybersicherheitsagenda des BMI, S. 10) im Bereich der Beschaffung von IT-Sicherheitsprodukten für die Bundesverwaltung zu verankern, und wenn ja, welche?

Kompetenzen eines etwaigen einzurichtenden CISO Bund sind Teil der laufenden Abstimmung des Referentenentwurfs des „Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG). Unabhängig davon sieht das BSI-Gesetz bereits heute Pflichten des BSI bzgl. der Bereitstellung und Nutzung von IT-Sicherheitsprodukten vor (siehe z. B. § 3 Absatz 1 Nummer 11 sowie § 8 Absatz 3 BSIG).

7. Unter welchen Umständen und Bedingungen hinsichtlich Erfüllung von CC, Reputation, Inhaberstruktur und Firmensitz des Herstellers darf eine Bundesbehörde eine produktscharfe Ausschreibung für ein IT-Sicherheitsprodukt an einen Hersteller mit Sitz außerhalb der Europäischen Union (EU) vornehmen?

Öffentliche Auftraggeber müssen bei der Leistungsbeschreibung den Grundsatz der Produktneutralität beachten. Diesem Grundsatz zufolge darf in der Leistungsbeschreibung nicht auf eine bestimmte Produktion oder Herkunft oder ein besonderes Verfahren, das die Erzeugnisse oder Dienstleistungen eines bestimmten Unternehmens kennzeichnet, oder auf gewerbliche Schutzrechte, Typen oder einen bestimmten Ursprung verwiesen werden, wenn dadurch bestimmte Unternehmen oder Produkte begünstigt oder ausgeschlossen werden (siehe § 31 Abs. 6 Satz 1 der Verordnung über die Vergabe öffentlicher Aufträge). Als Ausnahme vom genannten Grundsatz ist eine produktscharfe Ausschreibung dann zulässig, wenn sie durch den Auftragsgegenstand sachlich gerechtfertigt ist. Eine Rechtfertigung durch den Auftragsgegenstand setzt voraus, dass der Auftraggeber nachvollziehbare, objektive und auftragsbezogene Gründe für die produktscharfe Ausschreibung vorbringt und die Bestimmung folglich willkürfrei getroffen worden ist, solche Gründe tatsächlich vorhanden sind und die Bestimmung andere Wirtschaftsteilnehmer nicht diskriminiert, indem sie den Wettbewerb künstlich einschränkt. Sofern die in der Frage genannten

Kriterien im Einzelfall diesen Rechtfertigungsanforderungen genügen, ist eine produktscharfe Ausschreibung zulässig.

8. Gelten für IT-Sicherheitsprodukte von Herstellern mit Sitz außerhalb der EU dieselben Zertifizierungs- und Zulassungsregularien des BSI wie für Hersteller von IT-Sicherheitsprodukten mit Sitz innerhalb der EU?

Die Zulassungsregularien sind für alle beteiligten Parteien in der Technischen Leitlinie BSI TL – IT 01 „Mitwirkungspflichten in Zulassungsverfahren“ beschrieben, eine Unterscheidung nach Sitz des Herstellers gibt es dort nicht. Auch bei der Zulassung der IT-Sicherheitsprodukte zum Schutz von EU- bzw. NATO-CI (classified information) wird in den einschlägigen Regularien nicht zwischen in- und ausländischen Herstellern unterschieden.

Für die CC-Zertifizierung gelten für IT-Sicherheitsprodukte von Herstellern mit Sitz außerhalb der EU dieselben Zertifizierungsregularien des BSI wie für Hersteller von IT-Sicherheitsprodukten mit Sitz innerhalb der EU. Das Bundesministerium des Innern und für Heimat kann eine Zertifikatserteilung im Einzelfall untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen (§ 9 Absatz 4a BSIG).

9. Für welche IT-Sicherheitsprodukte wurden seit März 2022 Zertifizierungen für den Einsatz in der Bundesverwaltung nach welchem Zertifizierungsschema beim BSI beantragt, bei welchen davon wurde eine positive Zertifizierungsaussage getroffen, und bei welchen davon befand sich der Hauptsitz des Herstellers des IT-Sicherheitsprodukts außerhalb der EU (bitte nach Produktname, Art der beantragten Zertifizierung, Zertifizierungsaussage, Hersteller, Hauptsitz des Herstellers aufschlüsseln) für

   a) IT-Sicherheitsprodukte des Produkttyps Firewall,

   b) IT-Sicherheitsprodukte des Produkttyps Datendiode,

   c) IT-Sicherheitsprodukte des Produkttyps VS Guard,

   d) IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung,

   e) IT-Sicherheitsprodukte des Produkttyps Hypervisor,

   f) IT-Sicherheitsprodukte des Produkttyps Separation Kernel,

   g) IT-Sicherheitsprodukte des Produkttyps Mobile Device Management,

   h) IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement,

   i) IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente,

   j) IT-Sicherheitsprodukte des Produkttyps Key-Management-Software,

   k) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme,

   l) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme,

   m) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen,

   n) IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung,

   o) IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung,

p) IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger,

q) IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung,

r) IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung,

s) IT-Sicherheitsprodukte des Produkttyps Funkgeräte,

t) IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung,

u) IT-Sicherheitsprodukte des Produkttyps VPN-Client,

v) IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung,

w) IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger,

x) IT-Sicherheitsprodukte des Produkttyps VPN-Gateway,

y) IT-Sicherheitsprodukte des Produkttyps Datenschleusen (optional auch mit Datenwäschekomponente),

z) IT-Sicherheitsprodukte Verschlüsselung Layer 1,

aa) IT-Sicherheitsprodukte Verschlüsselung Layer 2,

bb) IT-Sicherheitsprodukte des Produkttyps Intrusion Detection System,

cc) IT-Sicherheitsprodukte Threat Detection System?

Die Zertifizierung nach den CC (Common Criteria), BSZ (Beschleunigte Sicherheitszertifizierung) und NESAS (Network Equipment Security Assurance Scheme) geschieht auf Herstellerantrag ohne Konkretisierung des Einsatzzwecks. Sofern die Hersteller einer Veröffentlichung zugestimmt haben, werden laufende Zertifizierungsverfahren auf der Webseite des BSI veröffentlicht. Das gleiche gilt für abgeschlossene Zertifizierungsverfahren.

Darüber hinaus bietet das BSI für die unter a) bis cc) aufgeführten Produktkategorien keine Zertifizierungsverfahren nach Technischen Richtlinien an, deshalb wurden in diesen Bereichen auch keine Produkte seit März 2022 nach technischen Richtlinien zertifiziert.

Es wird ergänzend auf die Antwort zu Frage 12 verwiesen.

10. Für welche IT-Sicherheitsprodukte wurden seit März 2022 Zulassungen für den Einsatz in der Bundesverwaltung durch welchen behördlichen Anwender beim BSI beantragt, bei welchen davon wurde eine positive Zulassungsaussage getroffen, und bei welchen davon befand sich der Hauptsitz des Herstellers des IT-Sicherheitsprodukts außerhalb der EU (bitte nach Produktname, beantragendem behördlichen Anwender samt des ihm zuzuordnenden Geschäftsbereichs der Bundesregierung, Zulassungsaussage, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln) für

a) IT-Sicherheitsprodukte des Produkttyps Firewall,

b) IT-Sicherheitsprodukte des Produkttyps Datendiode,

c) IT-Sicherheitsprodukte des Produkttyps VS Guard,

d) IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung,

e) IT-Sicherheitsprodukte des Produkttyps Hypervisor,

f) IT-Sicherheitsprodukte des Produkttyps Separation Kernel,

g) IT-Sicherheitsprodukte des Produkttyps Mobile Device Management,

h) IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement,

i) IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente,

j) IT-Sicherheitsprodukte des Produkttyps Key-Management-Software,

k) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme,

l) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme,

m) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen,

n) IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung,

o) IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung,

p) IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger,

q) IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung,

r) IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung,

s) IT-Sicherheitsprodukte des Produkttyps Funkgeräte,

t) IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung,

u) IT-Sicherheitsprodukte des Produkttyps VPN-Client,

v) IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung,

w) IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger,

x) IT-Sicherheitsprodukte des Produkttyps VPN-Gateway,

y) IT-Sicherheitsprodukte des Produkttyps Datenschleusen (optional auch mit Datenwäschekomponente),

z) IT-Sicherheitsprodukte Verschlüsselung Layer 1,

aa) IT-Sicherheitsprodukte Verschlüsselung Layer 2,

bb) IT-Sicherheitsprodukte des Produkttyps Intrusion Detection System,

cc) IT-Sicherheitsprodukte Threat Detection System?

Die Antwort kann der beigefügten Übersicht (Anlage 1) entnommen werden.*

Da es sich bei den Aufzählungspunkten d), y), bb) und cc) nicht um Produkttypen des VS-Produktkataloges gemäß § 52 VSA handelt, kann die Bundesregierung dazu keine Aussage treffen.

11. Für welche IT-Sicherheitsprodukte hat die Bundesverwaltung inklusive der IT-Dienstleister des Bundes für welchen behördlichen Anwender der Bundesverwaltung inklusive der IT-Dienstleister des Bundes seit März 2022 Verträge zur Beschaffung von IT-Sicherheitsprodukten geschlossen (bitte nach Produktname, Geschäftsbereich der vertragsschließenden Bundesbehörde, bedarfstragendem behördlichen Anwender, Art der Zertifizierung beziehungsweise Zulassungsaussage des beschafften IT-Sicherheitsprodukts, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln) für

a) IT-Sicherheitsprodukte des Produkttyps Firewall,

b) IT-Sicherheitsprodukte des Produkttyps Datendiode,

c) IT-Sicherheitsprodukte des Produkttyps VS Guard,

* Von einer Drucklegung der Anlage wird abgesehen. Diese ist auf Bundestagsdrucksache 20/8707 auf der Internetseite des Deutschen Bundestages abrufbar.

d) IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung und Abwehr,

e) IT-Sicherheitsprodukte des Produkttyps Hypervisor,

f) IT-Sicherheitsprodukte des Produkttyps Separation Kernel,

g) IT-Sicherheitsprodukte des Produkttyps Mobile Device Management,

h) IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement,

i) IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente,

j) IT-Sicherheitsprodukte des Produkttyps Key-Management-Software,

k) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme,

l) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme,

m) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen,

n) IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung,

o) IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung,

p) IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger,

q) IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung,

r) IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung,

s) IT-Sicherheitsprodukte des Produkttyps Funkgeräte,

t) IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung,

u) IT-Sicherheitsprodukte des Produkttyps VPN-Client,

v) IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung,

w) IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger,

x) IT-Sicherheitsprodukte des Produkttyps VPN-Gateway,

y) IT-Sicherheitsprodukte des Produkttyps Datenschleusen (optional auch mit Datenwäschekomponente),

z) IT-Sicherheitsprodukte Verschlüsselung Layer 1,

aa) IT-Sicherheitsprodukte Verschlüsselung Layer 2,

bb) IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 3,

cc) IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 4,

dd) IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 7,

ee) IT-Sicherheitsprodukte des Produkttyps Web Application Firewall,

ff) IT-Sicherheitsprodukte des Produkttyps Email Security Gateway,

gg) IT-Sicherheitsprodukte des Produkttyps EDR (Endpoint Detection and Response), NDR (Network Detection and Response), XDR (Extended Detection and Response), Device/Port/Schnittstellenkontrolle, UTM (unified Threat Management), Backup/Recovery, DLP (Data Loss Prevention), Archivierung, ersetzendes Scannen, TR-ESOR Langzeitarchivierung, Labeling und APT-Abwehr (APT = Advanced Persistent Threat), ISMS (Information Security Management System) und SIEM (Security Information and Event Management),

hh) IT-Sicherheitsprodukte Threat Detection System?

Auf die Vorbemerkung der Bundesregierung wird verwiesen. Die Beantwortung der Frage erfolgt eingestuft als „VS – Nur für den Dienstgebrauch“ gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA).* Die Informationen können der Anlage 2 entnommen werden.

12. Bei welchen der in Frage 11 erfragten IT-Sicherheitsprodukte befand sich der Hauptsitz des Herstellers des IT-Sicherheitsprodukts außerhalb der EU (bitte analog zu Frage 11 nach Produktname, Hersteller, Hauptsitz des Herstellers aufschlüsseln)?

Für die vom Beschaffungsamt zentral abgeschlossenen Rahmenverträge befindet sich der jeweilige Hauptsitz des Herstellers innerhalb der EU. Sofern der Hauptsitz des Herstellers für den Einsatz eines IT-Sicherheitsprodukts relevant ist, findet eine Einzelfallbetrachtung statt und wird nicht zentral vorgehalten. Darüber hinaus wird auf die öffentlich zugänglichen Quellen zum Hauptsitz der unterschiedlichen Hersteller verwiesen.

13. Welche Form des Vergabeverfahrens (z. B. Teilnahmewettbewerb, EU-weite Ausschreibung, freihändige Vergabe, produktscharfe Ausschreibung, Vergabeverordnung Verteidigung und Sicherheit – VSVgV) wurde jeweils für die in Frage 11 erfragten IT-Sicherheitsprodukte gewählt, und wann war der jeweils letzte Zeitpunkt für die Ausschreibung für das jeweilige IT-Sicherheitsprodukt (bitte analog zu Frage 11 nach Produktnamen, gewähltem Vergabeverfahren, Zeitpunkt der letzten Ausschreibung aufschlüsseln)?

Für die zentral vom Beschaffungsamt geschlossenen Verträge war das Vergabeverfahren jeweils ein Verhandlungsverfahren ohne Teilnahmewettbewerb nach VSVgV mit dem Hersteller des Produkts. Das jeweilige Datum des letzten Verhandlungsverfahrens kann der Anlage 3 entnommen werden.**

14. Welche der in Frage 11 erfragten IT-Sicherheitsprodukte kommen seit Vertragsschluss zur Beschaffung in der Bundesverwaltung bei welchem behördlichen Anwender jeweils tatsächlich zum Einsatz, und für welche der in Frage 11 erfragten IT-Sicherheitsprodukte wurden nach Vertragsschluss zur Beschaffung keine Abrufe durch die Bundesverwaltung getätigt (bitte analog zu Frage 11 aufschlüsseln)?

15. Wie hoch ist jeweils die Anzahl der Behörden, die die in Frage 11 erfragten IT-Sicherheitsprodukte in ihrer Verwaltung verwenden (bitte analog zu Frage 11 nach Produktnamen, Anzahl verwendender Bundesbehörden inklusive IT-Dienstleister des Bundes und dem ihr zuzuordnenden Geschäftsbereich der Bundesregierung aufschlüsseln)?

16. Wie hoch ist jeweils die Anzahl der Lizenzen für die in Frage 11 erfragten IT-Sicherheitsprodukte, die die Bundesverwaltung inklusive der IT-Dienstleister des Bundes für welchen behördlichen Anwender der Bun-

* Das Bundesministerium des Innern und für Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

** Von einer Drucklegung der Anlage wird abgesehen. Diese ist auf Bundestagsdrucksache 20/8787 auf der Internetseite des Deutschen Bundestages abrufbar.

desverwaltung inklusive der IT-Dienstleister des Bundes jeweils bezogen hat (bitte analog zu Frage 11 nach Produktnamen, produktverwendenden Bundesbehörden, zuzuordnendem Geschäftsbereich der Bundesregierung und jeweiliger Anzahl der Produktlizenzen aufschlüsseln)?

17. Wie hoch ist jeweils die Anzahl der Installationen der in Frage 11 erfragten IT-Sicherheitsprodukte in den jeweils produktverwendenden Bundesbehörden inklusive der IT-Dienstleister des Bundes (bitte analog zu Frage 11 nach Produktnamen, produktverwendenden Bundesbehörden, zuzuordnendem Geschäftsbereich der Bundesregierung und jeweiliger Anzahl der Installationen aufschlüsseln)?

Die Fragen 14 bis 17 werden zusammen beantwortet.

Auf die Vorbemerkung der Bundesregierung wird verwiesen. Die Beantwortung der Fragen erfolgt eingestuft in Anlage 2 als „VS – Nur für den Dienstgebrauch“ gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA).*

18. Wie stellt sich bei den in Frage 11 erfragten IT-Sicherheitsprodukten nach Kenntnis der Bundesregierung die Lieferkette hinsichtlich Transparenz von Inhaberstruktur und Firmensitz (nach Veröffentlichung der Panama Papers vom Bund gefordert) jeweils dar (bitte analog zu Frage 11 jeweils nach Produktnamen, Produkthersteller, Produktintegrator, Produktbetrieb, Produktwartung, Produktlieferant aufschlüsseln)?

Bei bisher im Zulassungsschema unbekannten Unternehmen kann vor Aufnahme eines Zulassungsverfahrens eine Unternehmensauskunft zur Klärung von Firmensitz und Inhaberstruktur eingeholt werden. Falls gesetzlich gefordert, wird das BSI durch das BAFA in den Bewertungsprozess von Übernahmen eingebunden. Weitere Aspekte der Lieferketten-Sicherheit werden im Rahmen von Zulassungsverfahren lediglich in allgemeiner Weise betrachtet. Unter Nutzung und auf Basis der Common Criteria sind dabei Teilaspekte wie z. B. die Festschreibung eines definierten Konstruktionsstandes, Sicherheit der Entwicklungsstandorte, definierte Fehlerbehebungsprozesse und Auslieferungsverfahren Gegenstand der Betrachtungen.

19. Welche und wie viele der in der Antwort zu Frage 11 genannten Hersteller sind über welchen Zeitraum geheimschutzbetreut nach SÜG?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

Die Beantwortung der Frage nach den durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) nach dem Sicherheitsüberprüfungsgesetz (SÜG) geheimschutzbetreuten Hersteller erfolgt eingestuft als „VS – Nur für den Dienstgebrauch“ gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA).*

* Das Bundesministerium des Innern und für Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

20. Für wie viele Mitarbeiterinnen und Mitarbeiter von Herstellern von IT-Sicherheitsprodukten, deren IT-Sicherheitsprodukte in der Bundesverwaltung inklusive der IT-Dienstleister des Bundes, zum Einsatz kommen, wurde ein Sicherheitsüberprüfungsverfahren gemäß Sicherheitsüberprüfungsgesetz durchgeführt (bitte nach Land des Sitzes des Herstellers der sicherheitsüberprüften Mitarbeiterinnen und Mitarbeiter aufschlüsseln)?

Für die vom BMWK geheimschutzbetreuten Hersteller von IT-Sicherheitsprodukten (s. Antwort zu Frage 19) wurden 11 879 Sicherheitsüberprüfungsverfahren gemäß SÜG durchgeführt.

Diese Anzahl orientiert sich nicht spezifisch an den Aufträgen zur Herstellung von IT-Sicherheitsprodukten, sondern an dem Gesamt-VS-Auftragsvolumen des jeweiligen Unternehmens. Der Sitz der genannten geheimschutzbetreuten Unternehmen befindet sich in Deutschland.

21. Betrachtet die Bundesregierung Technologien im Bereich der Cybersicherheit als Schlüsseltechnologien?

a) Wenn ja, welche Technologien im Bereich der Cybersicherheit sind das genau?

b) Wenn nein, plant die Bundesregierung, Technologien im Bereich der Cybersicherheit als Schlüsseltechnologien zu definieren, und welche genau?

Die Fragen 21 bis 21b werden gemeinsam beantwortet.

Aus Sicht des Zulassungsschemas werden solche Technologien als Schlüsseltechnologien angesehen, deren Funktionstüchtigkeit für die Handlungsfähigkeit der Bundesrepublik Deutschland entscheidend sind. Hierbei umfassen die Schlüsseltechnologien die Bereiche Prävention, Detektion und Reaktion.

Im Rahmen der Regelungen des materiellen Geheimschutzes sind für die Prävention die dabei zu verwendenden VS-IT-Systeme entscheidend, da sie Maßnahmen zur Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität von elektronischen Verschlusssachen umsetzen.

Verankert wird der Schlüsselcharakter gemäß § 52 VSA im VS-Produktkatalog des BSI durch die Festlegung der Zulassungsrelevanz und die Spezifikation sicherheitsfunktionaler Anforderungen (VS-Anforderungsprofile).

Insbesondere die folgenden Schlüsseltechnologien als Teil der präventiven Maßnahmen werden aus Sicht des BSI-Zulassungsschemas als zentral gesehen:

- Kryptographische Verfahren und Protokolle als Basistechnologie für verschiedenste Anwendungsszenarien
- Netzwerkkopplung und vertrauenswürdige Übertragungsverschlüsselung
- Sicheres mobiles oder ultramobiles Arbeiten
- Sichere Funk- und Satellitenkommunikation

Weitere Schlüsseltechnologien ergänzen die Vorgaben aus § 52 VSA und dem VS-Produktkatalog des BSI, indem sie unverzichtbar sind für die Detektion von Cyber-Angriffen. Dies betrifft Technologien, mit denen Cyber-Angriffe verhaltensbedingt durch Auswertung von Protokolldaten mit Hilfe innovativer Verfahren (u. a. KI, Sandboxanalyse) detektiert, gestoppt und analysiert werden können, wie z. B.

- EDR (Endpoint Detection and Response),
- NDR (Network Detection and Response) und

- XDR (eXtended Detection and Response).

Zur Reaktion auf Cyberangriffe gehören Produkte zum Schwachstellenmanagement zu Schlüsseltechnologien. Unter Schwachstellenmanagement wird in diesem Zusammenhang nicht nur das reine Scannen nach bekannten Schwachstellen verstanden, sondern auch das Monitoring von IT-Systemen, Policy-Prüfungen und die automatisierte Verarbeitung von CERT-Bund-Meldungen und -Advisories.

22. Welches Ressort der Bundesregierung wird federführend für die Erfüllung des in der Nationalen Sicherheitsstrategie festgestellten Bedarfs eines „[…] gezielten Auswahlprozesses, der Wissensentwicklung und -verbreitung, der Rahmensetzung, der Ressourcenmobilisierung und Marktentwicklung für strategische Technologielinien“ (Nationale Sicherheitsstrategie, Bundestagsdrucksache 20/7220, S. 57) zuständig sein?

23. Welche strategischen Technologielinien im Zusammenhang mit digitaler Souveränität meint die Bundesregierung genau (bitte vollständig aufzählen)?

24. Was meint die Bundesregierung genau mit dem Auswahlprozess zu strategischen Technologielinien?

25. Welche Kriterien legt die Bundesregierung in diesem Auswahlprozess zur konkreten Auswahl der strategischen Technologielinien an?

Die Fragen 22 bis 25 werden zusammen beantwortet.

Die Bundesregierung verfolgt ein Konzept der Integrierten Sicherheit, wie in der Nationalen Sicherheitsstrategie angelegt. Integrierte Sicherheit steht für das Zusammenwirken aller relevanten Akteure, Mittel und Instrumente mit dem Ziel, die Sicherheit Deutschlands umfassend zu erhalten und zu stärken. Das Konzept ist für die Umsetzung der Nationalen Sicherheitsstrategie sowie der dort verankerten weiteren Strategien handlungsleitend. Die Bundesregierung wird sich konstant auf allen Ebenen zwischen den Ressorts abstimmen. Die Bundesregierung beabsichtigt zudem, den Deutschen Bundestag regelmäßig über den Stand der Umsetzung zu unterrichten.

Zur Umsetzung der Nationalen Sicherheitsstrategie wird im Weiteren auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/8029 verwiesen.

Die Beiträge zu einer Strategie zum Schutz und Förderung von Technologie und Innovation werden entlang der jeweiligen Ressortzuständigkeiten erarbeitet. Im Rahmen der interministeriellen Zusammenarbeit werden weitere Ressorts gemäß ihrer Zuständigkeit beteiligt.

Das in der Nationalen Sicherheitsstrategie formulierte Ziel, technologische und digitale Souveränität durch einen gezielten Auswahlprozess, Wissensentwicklung und -verbreitung, Rahmensetzung, Ressourcenmobilisierung und Marktentwicklung für strategische Technologielinien zu erzielen, wird in der Strategie konkretisiert. Die Nationale Sicherheitsstrategie stellt allerdings keinen Schlusspunkt dar. Sie soll vielmehr einen kontinuierlichen Prozess zur Stärkung der Sicherheit Deutschlands befördern und einen Ansatzpunkt für den Umgang mit künftigen Technologien und Innovationen bieten. Aufgrund dessen kann keine vollständige und abschließende Auflistung strategischer Technologielinien im Zusammenhang mit digitaler Souveränität erfolgen. Erste konkrete Maßnahmen und Kriterien werden im laufenden Umsetzungsprozess entlang der jeweiligen Ressortzuständigkeiten erarbeitet.

26. Welche Förderprogramme der Bundesregierung zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität liefen und laufen seit dem Jahr 2018 (bitte jeweils die finanzielle Ausstattung jeweils für die Jahresscheiben von 2018 bis 2023 nennen)?

Die Ausstattungen sind für die Jahre 2018 bis 2024 wie folgt:

Zum Förderprogramm Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“ (2015 bis 2020)

Ausstattung 2018	**Ausstattung 2019**	**Ausstattung 2020**	**Ausstattung 2021**	**Ausstattung 2022**	**Ausstattung 2023**
45.784.984 €	47.529.929 €	54.281.763 €	67.631.787 €	50.387.154 €	37.202.228 €

Zum Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ (2021 bis 2026)

Ausstattung 2021	**Ausstattung 2022**	**Ausstattung 2023**
9.521.400 €	45.483.673 €	100.597.772 €

Zum Förderprogramm für Forschungs- und Entwicklungsvorhaben im Bereich „Cybersicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G“ im Rahmen des „45. Elements“ des Konjunkturprogramms der Deutschen Bundesregierung zur Adressierung der Folgen der Corona-Pandemie

Ausstattung 2022	**Ausstattung 2023**	**Ausstattung 2024**
14.800.000 €	20.635.000 €	23.450.000 €

27. Plant die Bundesregierung derzeit, neue Förderprogramme zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität aufzulegen, und wenn ja, wie hoch wird die von der Bundesregierung angedachte finanzielle Ausstattung sein?

Das aktuelle Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ läuft noch bis Ende 2026. Im Rahmen des Programms werden regelmäßig neue Fördermaßnahmen gestartet. Weitere Förderprogramme zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität sind zurzeit nicht geplant.

28. Welche Veranstaltungen der Bundesregierung (Gipfel, Wettbewerbe, Hackathons) zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität wurden seit dem Jahr 2018 organisiert und durchgeführt (bitte nach Veranstaltungsformat, Veranstaltung und Veranstaltungstermin aufschlüsseln)?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Termin	**Veranstaltung**	**Veranstaltungsformat**
30.09.2020	CIC-Thementag: „Blockchain in der öffentlichen Verwaltung“	Online-Veranstaltung (Webinar)
14.01.2021	CIC-Thementag: „Security by agile Design“	Online-Veranstaltung (Webinar)
10.05.2021	Partner-Forum des BAMF „Förderale Blockchain Infrastruktur Asyl (FLORA)“ beim Digitalen Staat	Kongress
01.07.2021	CIC-Thementag: „Self-Sovereign Identity (SSI)“	Online-Veranstaltung (Webinar)

Termin	**Veranstaltung**	**Veranstaltungsformat**
28.10.2021	CIC-Thementag: Das Datennetzwerkprotokoll IPv6 und dessen Auswirkungen auf die IT	Online-Veranstaltung (Webinar)
Seit 31.3.2022	„Grand Challenge der Quantenkommunikation“ im Rahmen des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit	Wettbewerb
12.05.2022	CIC-Thementag: „Self-Sovereign Identity (SSI) – selbstbestimmtes digitales Management“	Online-Veranstaltung (Webinar)
09.09.2022	Partner bei der Blockchain@HTW Conference 2022 „Das Web 3.0: Das Metaverse sind wir! Die Blockchain-Technologie als Rückgrat von Metaverse und Web3.0“ inklusive Vortrag „Einblicke in die Pilotierung der Föderalen Blockchain Infrastruktur Asyl (FLORA)“	Online-Veranstaltung (Konferenz)
28.2. – 26.3.2023	Informationstour zum Thema IT-Sicherheitsforschung durch Schulen und Museen im Rahmen der Kommunikationsinitiative „Sichere die digitale Zukunft!“	Informationstour
1.5. – 31.10.2023	OZG-Security-Challenge 2023	Verwaltungsinterne Challenge mit Begleitmaßnahmen zur Wissensentwicklung und -verbreitung
13. – 15.3.2023	Nationale Konferenz IT-Sicherheitsforschung 2023	Konferenz
25.04.2023	Fachforum „FLORA – Status des Projektes Föderale Blockchain-Infrastruktur Asyl“ beim Digitalen Staat	Kongress
26.04.2023	Fachforum „Digitale Identitäten / Digitale Signaturen – Vorreiterrolle BAMF“ beim Digitalen Staat	Kongress
10./11. Mai 2023	Jährlicher BSI IT-Sicherheitskongress	Kongress
2023	Partner bei der Small-States meet Blockchain@HTW Conference 2023 „Small States–Big Issues: Can Technology be the rescue(r)? inklusive Vortrag „: Benefits of Self-Sovereign Identity in Public Administration“	Konferenz
	Regelmäßige Live-Hackings (zweimal im Jahr) für Studierende und Beschäftigte	Präsenzveranstaltungen

29. Welche Veranstaltungen plant die Bundesregierung derzeit im thematischen Zusammenhang mit der Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Termin	**Veranstaltung**	**Veranstaltungsformat**
7./8. Mai 2024	Jährlicher IT-Sicherheitskongress	Kongress/digital
28.09.2023	CIC-Thementag: „IT-Security & Zero-Trust“	Online-Veranstaltung (Webinar)
30.11.2023	CIC-Thementag: „Digitale Souveränitat“	Online-Veranstaltung (Webinar)
November 2023	Informationssicherheitstag	
Regelmäßige Live-Hackings (zweimal im Jahr) für Studierende und Beschäftigte	Präsenzveranstaltungen	Vorträge & Infostände und Hacker-Präsentation

30. Welche Kooperationen mit Universitäten und Hochschulen pflegt die Bundesregierung zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Ressorts	**Behörde/ Einrichtung**	**Kooperation mit folgender Universität/ Hochschule**
BMG	BfArM	Beirat im Cyber Security Cluster Bonn, darüber Kooperation mit Hochschule Bonn-Rhein-Sieg, Hochschule des Bundes für öffentliche Verwaltung, Hochschule Niederrhein.
BMBF		Die Bundesregierung fördert gemeinsam mit den Bundesländern das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE sowie das CISPA Helmholtz-Zentrum für Informationssicherheit als Zentren der Forschung in Sicherheitstechnologien sowie des Wissens- und Technologietransfers. Darüber hinaus fördert die Bundesregierung gemeinsam mit den Bundesländern den Fraunhofer-Fachhochschulverbund „Lernlabor Cybersicherheit“ bestehend aus Fraunhofer-Instituten, Fachhochschulen und der Fraunhofer Academy. Das Lernlabor entwickelt hochwertige Weiterbildungen zum Thema Cybersicherheit mit dem Ziel, aktuelles Forschungswissen praxisnah und anwendungsorientiert in Wirtschaft und Gesellschaft zu transferieren. Durch eine breit aufgestellte Projektförderung unterstützt die Bundesregierung zudem die zu Sicherheitstechnologien forschenden Hochschulen und Forschungseinrichtungen in ihren Forschungsprojekten sowie bei der Wissensentwicklung, Aus- und Weiterbildung von Fachkräften und Wissenschaftskommunikation.
BSI		Zusammenarbeit in Projekten und zur Ausbildung von Studierenden. Hintergrundinformationen (Auswahl von Universitäten). • Hochschule Bonn-Rhein-Sieg • Hochschule des Bundes • Universität der Bundeswehr • Ruhr Universität Bochum • FH Münster • Westfälische Hochschule • Universität Potsdam • Universität Saarbrücken • Karlsruher Institut für Technologie (KIT) • TU Darmstadt • TU München • Goethe-Universität Frankfurt • Hochschule Darmstadt • Universität Siegen

31. Welche Kooperationen mit öffentlichen Forschungseinrichtungen pflegt die Bundesregierung zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Ressorts	**Behörde/ Einrichtung**	**Kooperation mit folgender öffentlicher Forschungseinrichtung**
BMEL	BVL	BMEL ressortweit; Kollaboration im Zusammenhang der Projektarbeit zu KIDA, in der u. a. die digitale Infrastruktur für die Arbeit mit KI entwickelt werden soll.
BMG	BfArM	Beirat im Cyber Security Cluster Bonn, darüber Kooperation mit Fraunhofer IAIS/SIT/FKIE
BMBF		siehe Antwort zu Frage 30
BSI		Verschiedenste Kooperationen zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität mit renommierten öffentlichen Forschungseinrichtungen. Hintergrundinformationen: • Agentur für Innovation in der Cybersicherheit (Cyberagentur) • Bundesagentur für Sprunginnovationen (SPRIND) • Forschungsinstitut CODE (FI CODE) • KASTEL • DLR • Horst-Görtz-Institut • Max-Planck-Gesellschaft (MPG) • Helmholtz-Gemeinschaft • Fraunhofer-Gesellschaft • Leibniz-Gemeinschaft • Deutsche Forschungsgemeinschaft • CISPA Helmholtz-Zentrum • Institut für Internet-Sicherheit • Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) • Open CoDE (Plattform der Öffentlichen Verwaltung für den Austausch von Open Source Software) und weitere

32. Welche Kooperationen mit privaten Forschungseinrichtungen pflegt die Bundesregierung zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Behörde/Einrichtung	**Kooperation mit folgender privater Forschungseinrichtung**
BSI	Verschiedenste Kooperationen zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität mit renommierten privaten Forschungseinrichtungen. • Hasso-Plattner-Institut • Steinbeis Innovation GmbH bzw. ausführende Stelle Steinbeis Europa Zentrum • Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)

33. In Höhe welcher Summe sind finanzielle Mittel im Bundeshaushalt 2023 zur Erforschung und Entwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität hinterlegt (bitte nach Einzelplan, Kapitel und Titel aufschlüsseln)?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Einzelplan	**Kapitel**	**Titel**	**Summe**	**Hinweis**
14	1404	551 04 (Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien)	24.650.000 €	Etat Cyberagentur
30	3004	683 20 (Kommunikationssysteme, IT-Sicherheit)	137.800.000 €	
06	02	544 02 (Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien)	24.650.000 €	Etat Cyberagentur
06	23	53204 (Behördenspezifische fachbezogene Verwaltungsausgaben)	3.282.600,30 €	
06	23	68602 (Zuschüsse zur Förderung der IT-Sicherheit)	13.399.659,76 €	

34. In Höhe welcher Summe sind finanzielle Mittel im Regierungsentwurf des Bundeshaushalts 2024 zur Erforschung und Entwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität enthalten (bitte nach Einzelplan, Kapitel und Titel aufschlüsseln)?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Einzelplan	**Kapitel**	**Titel**	**Summe**	**Hinweis**
14	1404	551 04 (Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien)	25.000.000 €	Etat Cyberagentur
30	3004	68320 (Kommunikationssysteme, IT-Sicherheit)	129.440.000 €	
06	0602	544 02 (Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien)	25.000.000 €	Etat Cyberagentur

35. Ist es gesetzlich und vergaberechtlich möglich, bestimmte Hersteller von IT-Sicherheitsprodukten aufgrund der Verortung ihres Hauptsitzes in einem bestimmten Land kategorisch von Auftragsvergaben im Bereich der IT-Sicherheitsprodukte für die Bundesverwaltung auszuschließen, und wenn nein, plant die Bundesregierung dahin gehende Rechtsänderungen oder würde diese unterstützen?

Das im deutschen Vergaberecht geltende Gleichbehandlungsgebot bzw. das damit korrespondierende Diskriminierungsverbot (siehe etwa § 97 Absatz 2 des Gesetzes gegen Wettbewerbsbeschränkungen [GWB]) verbieten jede unmittelbare und mittelbare Benachteiligung von Bietern aus dem Ausland. Eine Unterscheidung zwischen Unternehmen aus dem EU-Ausland und aus Drittstaaten trifft das deutsche Vergaberecht nicht. Ausnahmen von dem genannten Grundsatz müssen gesetzlich gestattet sein.

Ausnahmetatbestände, die unter bestimmten Voraussetzungen an die Herkunft der Bieter anknüpfen, finden sich in § 7 Absatz 2 ff. und § 4 Absatz 1 des Bundeswehrbeschaffungsbeschleunigungsgesetzes (BwBBG). Der Anwendungsbereich des BwBBG ist allerdings auf bestimmte Aufträge im Verteidigungsbereich beschränkt (siehe § 2 BwBBG) und zudem zeitlich befristet (siehe § 9 BwBBG). An die drittstaatliche Herkunft von Waren knüpft die Ausnahmevorschrift in § 55 der Sektorenverordnung an. Sicherheitsinteressen lassen sich im Übrigen allgemein nach § 107 Absatz 2 GWB i. V. m. Artikel 346 des Vertrages über die Arbeitsweise der Europäischen Union berücksichtigen. Im Rahmen der Erarbeitung des geplanten Vergabetransformationspakets prüft die Bundesregierung derzeit, inwieweit weitere Ausnahmetatbestände völker- und unionsrechtlich zulässig wären.

36. Sind bestimmte Hersteller von IT-Sicherheitsprodukten aufgrund der Verortung ihres Hauptsitzes in einem bestimmten Land kategorisch von Auftragsvergaben im Bereich der IT-Sicherheitsprodukte für die Bundesverwaltung ausgeschlossen, und wenn ja, um welche Länder handelt es sich dabei aus welchen Gründen?

Es gibt in Deutschland keine gesetzlichen Grundlagen für einen kategorischen Ausschluss von Herstellern aufgrund der Verortung ihres Hauptsitzes in einem bestimmten Land. Wenn Zweifel an der Vertrauenswürdigkeit eines Herstellers eines IT-Sicherheitsproduktes bestehen, werden zusätzliche Informationen eingeholt und in die Entscheidung mit einbezogen.

37. Plant die Bundesregierung, bestimmte Hersteller von IT-Sicherheitsprodukten aufgrund der Verortung ihres Hauptsitzes in einem bestimmten Land kategorisch von Auftragsvergaben im Bereich der IT-Sicherheitsprodukte für die Bundesverwaltung auszuschließen, und wenn ja, um welche Länder handelt es sich dabei aus welchen Gründen?

Auf die Antwort zu Frage 36 wird verwiesen.

38. Plant die Bundesregierung, einerseits im Zuge der vom BMI in seiner Cybersicherheitsagenda angekündigten Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und andererseits der von der Bundesregierung in ihrer Digitalstrategie angekündigten ganzheitlichen Stärkung des Cybersicherheitsökosystems für die zuständigen Cybersicherheitsbehörden umfangreiche Ausnahmen vom Beschaffungsrecht des Bundes vorzusehen, damit deutsche IT-Sicherheitsbehörden zur Erfüllung ihres Auftrags innerhalb kürzester Zeit neueste Technologien und Software für die IT-Sicherheit und die Cyberabwehr beschaffen können?

39. Plant die Bundesregierung, einerseits im Zuge der vom BMI in seiner Cybersicherheitsagenda angekündigten Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und andererseits der von der Bundesregierung in ihrer Digitalstrategie angekündigten ganzheitlichen Stärkung des Cybersicherheitsökosystems künftig bei IT-Beschaffungsvorhaben des Bundes einen bestimmten Anteil der Sachmittel für IT-Vorhaben des Bundes für Cybersicherheit aufzuwenden (wenn nein, bitte begründen)?

40. Plant die Bundesregierung, einerseits im Zuge der vom BMI in seiner Cybersicherheitsagenda angekündigten Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und andererseits der von der Bundesregierung in ihrer Digitalstrategie angekündigten ganzheitlichen Stärkung des Cybersicherheitsökosystems im Bereich der materiellen Ausrüstung in bestimmten Fällen den Anbieterkreis bei Vergaben von Aufträgen zur Beschaffung von IT-Sicherheitsprodukten auf nationale Lieferketten zu beschränken, und wenn ja, in welchen Fällen?

Die Fragen 38 bis 40 werden gemeinsam mit „Nein“ beantwortet.

Die Verwendung eines bestimmten Anteils an Sachmitteln bei IT-Vorhaben für Cybersicherheit ist Gegenstand der derzeitigen NIS2-Abstimmung.

41. Macht die Produktzertifizierung des BSI auch zukunftsbezogene Aussagen zur Sicherheit für Updates oder Patches eines zu zertifizierenden IT-Sicherheitsprodukts, und wenn nein, plant die Bundesregierung, dahin gehende Änderungen vorzunehmen?

Eine Produktzertifizierung nach CC macht keine zukunftsbezogenen Aussagen zur Sicherheit von Updates oder Patches. Änderungen an der Zertifizierung nach CC, die solche Aussagen ermöglichen, sind derzeit nicht geplant. Ein vereinfachter Prozess, um bestehende Zertifikate um Updates oder Patches zu erweitern, ist aktuell in Pilotierung.

Eine Produktzertifizierung nach Technischen Richtlinien macht keine zukunftsbezogenen Aussagen zur Sicherheit für Updates oder Patches. Änderungen an der Zertifizierung nach Technischen Richtlinien, die solche Aussagen ermöglichen, sind derzeit nicht geplant.

Die Produktzertifizierung nach BSZ und NESAS macht grundsätzlich keine zukunftsbezogenen Aussagen zur Sicherheit für Updates oder Patches eines zu zertifizierenden IT-Sicherheitsprodukts. Ein Zertifikat für ein (durch Updates oder Patches) geändertes Produkt wird im Programm BSZ generell und im Programm NESAS CCS-GI grundsätzlich auf dem Wege einer Rezertifizierung erteilt. Im Programm NESAS CCS-GI haben Antragsteller die Möglichkeit, für ihr zertifiziertes Produkt „geringfügige Aktualisierungen“, definiert als „Anpassungen von Sicherheitsfunktionen oder der Beschaffenheit des Produktes, die der Aufrechterhaltung oder Wiederherstellung der zertifizierten Sicherheitsleistung (als Summe der Sicherheitsaussagen der Produktevaluation) dienen oder die für die Sicherheitsleistung irrelevant sind“, an das BSI zu melden, zusam-

men mit einem Bericht zur Auswirkungsanalyse und dem Votum der sachverständigen Stelle, die das Produkt im Rahmen der Zertifizierung geprüft hat. Widerspricht die Zertifizierungsstelle nicht innerhalb von 30 Kalendertagen, so gilt das geringfügig aktualisierte Produkt ebenso wie das ursprüngliche Produkt über das bestehende Zertifikat zertifiziert. Innerhalb der benannten Widerspruchsfrist gilt das geringfügig aktualisierte Produkt insofern als vorläufig zertifiziert.

42. Welche Vergabekriterien im Zusammenhang mit nationalen Sicherheitsaspekten, die über die reine technologische Sicherheit hinausgehen, sind in Vergabeverfahren zu IT-Sicherheitsprodukten berücksichtigt beziehungsweise spielen dort eine Rolle?

Die Frage 42 wird mit den Antworten zu den dazugehörigen Unterfragen beantwortet.

a) Ist die Freiheit von sogenannten Backdoors (auch Hintertüren oder Trapdoors) ein Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten, und wenn nein, plant die Bundesregierung dahin gehende Änderungen?

Ja, bei entsprechenden IT-Beschaffungen ist die Freiheit von Backdoors aufgrund der verpflichtend zu verwendenden EVB-IT-Vertragsmuster ein Vergabekriterium, z. B. geregelt in den EVB-IT AGB Überlassung Typ A Nr. 2.3.

b) Ist die Vertrauenswürdigkeit hinsichtlich der Inhaberstruktur von Herstellern von IT-Sicherheitsprodukten ein Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten, und wenn nein, plant die Bundesregierung dahin gehende Änderungen?

Abgesehen von ggf. einschlägigen Sanktionsvorgaben gegenüber direkten Lieferanten und Subunternehmen ist die Inhaberstruktur von Herstellern auch generell teilweise ein Vergabekriterium bei Verfahren nach VSVgV. Zusätzlich werden im Rahmen der Eignungsprüfung im Kontext der Ausschlussgründe (§ 123/124 GWB) auch weitere Kriterien zur generellen Zuverlässigkeit von Herstellern geprüft.

c) Ist der Firmenhauptsitz von Herstellern von IT-Sicherheitsprodukten ein Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten, und wenn nein, plant die Bundesregierung dahin gehende Änderungen?

Sofern Gesetze oder Verordnungen existieren, werden diese als Kriterien im Vergabeverfahren berücksichtigt.

d) Ist die nachhaltige Geheimschutzbetreuung des Herstellers eines in der Bundesverwaltung verwendeten IT-Sicherheitsprodukts ein Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten, und wenn nein, plant die Bundesregierung dahin gehende Änderungen?

Die nachhaltige Geheimschutzbetreuung des Herstellers eines in der Bundesverwaltung verwendeten IT-Sicherheitsprodukts ist ein bei Bedarf gefordertes Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten.

e) Sind die Lieferketten eines Herstellers von IT-Sicherheitsprodukten ein Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten, und wenn nein, plant die Bundesregierung dahin gehende Änderungen?

Sofern Gesetze oder Verordnungen hierzu existieren, werden diese als Kriterien im Vergabeverfahren berücksichtigt.

Die Bundesregierung plant keine konkreten Änderungen zu den in den Antworten zu den Fragen 42a bis 42e genannten Punkten.

43. Welche Förderprogramme der Bundesregierung zur nationalen industriellen Marktentwicklung für Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität liefen und laufen seit dem Jahr 2018 (bitte jeweils die finanzielle Ausstattung jeweils für die Jahresscheiben von 2018 bis 2023 nennen)?

Die erbetenen Angaben können der nachstehenden Tabelle entnommen werden.

Ressort	**Name des Förderprogramms**	**Ausstattung 2018**	**Ausstattung 2019**	**Ausstattung 2020**
BMBF	Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“ (2015 bis 2020)	45.784.984 €	47.529.929 €	54.281.763 €
BPOL	KI-Strategie der Bundesregierung der Jahre 2018/2019			127.500 €

Ressort	**Name des Förderprogramms**	**Ausstattung 2021**	**Ausstattung 2022**	**Ausstattung 2023**
BMBF	Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“ (2015 bis 2020)	67.631.787 €	50.387.154 €	37.202.228 €
BMBF	Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ (2021 bis 2026)	9.521.400 €	45.483.673 €	100.597.772 €
BPOL	KI-Strategie der Bundesregierung der Jahre 2018/2019	137.500 €		
BSI	Das Bundesamt für Sicherheit in der Informationstechnik setzt als durchführende Stelle des BMI das Förderprogramm für Forschungs- und Entwicklungsvorhaben im Bereich „Cybersicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G“ im Rahmen des „45. Elements“ des Konjunkturprogramms der Deutschen Bundesregierung zur Adressierung der Folgen der Corona-Pandemie um.		14.800.000 €	2023: 20.635.000 € 2024: 23.450.000 €

44. Plant die Bundesregierung, derzeit neue Förderprogramme zur nationalen industriellen Marktentwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität aufzulegen, und wenn ja, wie hoch wird die von der Bundesregierung angedachte finanzielle Ausstattung sein?

Das aktuelle Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ läuft noch bis Ende 2026. Im Rahmen des Programms werden regelmäßig neue Fördermaßnahmen gestartet.

45. Welche Transferstellen, Cluster und Netzwerke hat die Bundesregierung für den Wissenstransfer von der Wissenschaft in die Industrie bezüglich Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität bisher eingerichtet (bitte immer Jahr der Einrichtung nennen)?

Die Bundesregierung fördert gemeinsam mit den Bundesländern das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE in Darmstadt sowie das CISPA Helmholtz-Zentrum für Informationssicherheit in Saarbrücken als Zentren der Forschung in Cybersicherheit sowie des Wissens- und Technologietransfers. An beiden Zentren sowie am Institut für Informationssicherheit und Verlässlichkeit KASTEL in Karlsruhe und an der Ruhr-Universität Bochum hat die Bundesregierung im Jahr 2018 Gründungsinkubatoren eingerichtet, die Forscherteams seitdem mit innovativen Gründungsideen bei der Weiterentwicklung ihrer Ideen bis zur unternehmerischen Umsetzung unterstützen.

Seit Ende 2022 fördert die Bundesregierung zudem das „Forschungsnetzwerk Anonymisierung für eine sichere Datennutzung“. Unter anderem in fünf Kompetenzclustern treiben Forscherinnen und Forscher die Entwicklung von Anonymisierungstechnologien voran, um den technischen Datenschutz zu verbessern und damit eine erhöhte digitale Souveränität und mehr datenbasierte Innovationen zu ermöglichen.

46. Plant die Bundesregierung derzeit, weitere Transferstellen, Cluster und Netzwerke für den Wissenstransfer von der Wissenschaft in die Industrie bezüglich Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität einzurichten, und wenn ja, welche?

Die Bundesregierung unterstützt jeglichen Austausch von Wissenschaft und Industrie bezüglich Sicherheitstechnologien. Hierzu gehören der Austausch mit diversen Universitären und außeruniversitären Forschungseinrichtungen. Eine Vielzahl an Transferstellen unterliegt der Zuständigkeit der Länder.

47. In Höhe welcher Summe sind finanzielle Mittel im Bundeshaushalt 2023 zur Marktentwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität hinterlegt (bitte nach Einzelplan, Kapitel und Titel aufschlüsseln)?

Auf die Antwort zu Frage 33 wird verwiesen.

48. In Höhe welcher Summe sind finanzielle Mittel im Regierungsentwurf des Bundeshaushalts 2024 zur Marktentwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität enthalten (bitte nach Einzelplan, Kapitel und Titel aufschlüsseln)?

Auf die Antwort zu Frage 34 wird verwiesen.

49. Welche Beratungs- und Transferstellen hat die Bundesregierung für die Bundesverwaltung zu Fragen der Beschaffung von IT-Sicherheitsprodukten eingerichtet (bitte immer Jahr der Einrichtung nennen)?

Für allgemeine Fragen von Bedarfsträgerinnen und Bedarfsträgern zur Beschaffung stellt das Beschaffungsamt des Bundes als zentraler Ausrüster für die öffentliche Verwaltung eine Vielzahl von Informationen zur Verfügung. Das BSI trägt durch seine Zulassungen und Zertifizierungen Gewähr für eine Auswahl an sicheren IT-Sicherheitsprodukten.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333

Anlage 1 zur Antwort auf Frage 10 der Kleinen Anfrage 20/8103

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Firewall	secunetSBC 6.1	secunet Security Networks AG	Freigabeempfehlung	BDBOS	EU
Firewall	genuate NdB WebRTC	genua GmbH	Einsatzerlaubnis	genua GmbH	EU
Firewall	secunetSBC 6.1	secunet Security Networks AG	Freigabeempfehlung	BDBOS	EU
Datendiode	Sina One Way H 1.0	secunet Security Networks AG	Freigabeempfehlung	DEUmilSAA	EU
Datendiode	SDoT Software Data Diode 1.3	INFODAS GmbH	Zulassung	DEUmilSAA	EU
VS-Guard	SECCOM® Secure Exchange Gateway (SEG) 4.2.1.0 (im Umfeld GIADS)	Airbus Defence and Space GmbH	Freigabeempfehlung	DEUmilSAA	EU
VS-Guard	SECCOM® Secure Exchange Gateway (SEG) 4.2.5.1.8.0 (im Umfeld SARah)	Airbus Defence and Space GmbH	Freigabeempfehlung	DEUmilSAA	EU
VS-Guard	SEG 4.2.5.1 (Anpassentwicklung ATTS (Ausbildungs- Trainings- und Testsystem) GIADS /KOFA)	Airbus Defence and Space GmbH	Freigabeempfehlung	DEUmilSAA	EU
VS-Guard	SDoT Security Gateway 6.1 Patch1	INFODAS GmbH	Einzelzulassung	DEUmilSAA	EU
VS-Guard	SECCOM® Secure Exchange Gateway (SEG) 5.x	Airbus Defence and Space GmbH	Zulassung	DEUmilSAA	EU
Hypervisor	SecuStack 21.06 (in der Ausprägung "SecuStack Titan“)	secunet Security Networks AG	Zulassung	Auswärtiges Amt	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Mobile Device Management, Sichere mobile Lösung	IdZ ES CHARON (Infanterist der Zukunft, Erweitertes System) 2.X (VJTF)	Rheinmetall Defence Electronic GmbH	Zulassung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	ED7-FN oSMS	Rohde & Schwarz SIT GmbH	Freigabeempfehlung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	ED7 oSMS für ED7-FN mit CApp SCIP	Rohde & Schwarz SIT GmbH	Freigabeempfehlung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	BBKME II	Thales Deutschland GmbH	Zulassung	BMVI	EU
Schlüsselspeicher-und Verteilkomponente	Keyserver 8.0	genua GmbH	Zulassung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	KPE III	Thales Deutschland GmbH	Zulassung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	"SMS SVFuA"	Rohde & Schwarz GmbH & Co. KG	Zulassung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	CCMU	Thales Deutschland GmbH	Zulassung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	DTD II	Thales Deutschland GmbH	Zulassung	DEUmilSAA	EU
Verschlüsselungsgerät für Satellitensysteme	SAR-Lupe Bodensegment	OHB System AG	Zulassung	DEUmilSAA	EU
Verschlüsselungsgerät für Satellitensysteme	H2Sat-GCU	OHB System AG	Zulassung	DEUmilSAA	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Verschlüsselungsgerät für Satellitensysteme	H2Sat-SSU	OHB System AG	Zulassung	DEUmilSAA	EU
Verschlüsselungsgerät für Satellitensysteme	PROOF mini PRS SM Receiver	Siemens AG	Zulassung	BMVI	EU
Verschlüsselungsgerät für Satellitensysteme	SARah (Phased Array)	DSI Informationstechnik GmbH	Zulassung	DEUmilSAA	EU
Dateiverschlüsselung (stand-alone)	Chiasmus_Kommandozeile_fuer_die_Bundeswehr	BSI - Bundesamt für Sicherheit in der Informationstechnik	Freigabeempfehlung	DEUmilSAA	EU
Dateiverschlüsselung (stand-alone)	Chiasmus_Linux_fuer_die_Bundeswehr	BSI - Bundesamt für Sicherheit in der Informationstechnik	Freigabeempfehlung	DEUmilSAA	EU
Dateiverschlüsselung (stand-alone)	Chiasmus_Kommandozeile_fuer_die_Bundeswehr	BSI - Bundesamt für Sicherheit in der Informationstechnik	Freigabeempfehlung	DEUmilSAA	EU
Dateiverschlüsselung (stand-alone)	Chiasmus_Linux_fuer_die_Bundeswehr	BSI - Bundesamt für Sicherheit in der Informationstechnik	Freigabeempfehlung	DEUmilSAA	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Dateiverschlüsselung (stand-alone)	Chiasmus_fuer_Windows_fuer_die_Schluesselerzeugung_bei_der_Bundeswehr	BSI - Bundesamt für Sicherheit in der Informationstechnik	Freigabeempfehlung	DEUmilSAA	EU
Festplattenverschlüsselung	SafeGuard Device Encryption	Sophos GmbH	Freigabeempfehlung	DEUmilSAA	EU
Festplattenverschlüsselung	R&S Trusted Storage Module	Rohde & Schwarz Cybersecurity GmbH	Zulassung	BMWK	EU
Festplattenverschlüsselung	R&S®Trusted Disk 3.X (Verwendung im IdZ ES - Führungsrechner, (VJTF) Very High Readiness Joint	Rohde & Schwarz Cybersecurity GmbH	Zulassung	DEUmilSAA	EU
Festplattenverschlüsselung	R&S®Trusted Disk 3.X (Verwendung im IdZ ES-Führungsrechner)	Rohde & Schwarz Cybersecurity GmbH	Zulassung	DEUmilSAA	EU
Festplattenverschlüsselung	Utimaco DiskEncrypt 9_00	Utimaco GmbH	Zulassung	DEUmilSAA	EU
Sicherer mobiler Datenträger	Kobra Drive VS und Kobra Stick VS 1.x	DIGITTRADE GmbH	Zulassung	BMWK	EU
Sicherer mobiler Datenträger	Kobra Drive VS und Kobra Stick VS 1.0	DIGITTRADE GmbH	Zulassung	BMWK	EU
Telefonverschlüsselung	ED7-FN mit CApp SCIP	Rohde & Schwarz SIT GmbH	Freigabeempfehlung	DEUmilSAA	EU
Telefonverschlüsselung	ED7-FN mit CApp SCIP	Rohde & Schwarz SIT GmbH	Freigabeempfehlung	DEUmilSAA	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Telefonverschlüsselung	TCU 7000 E 1.0	Elbit Systems Deutschland GmbH & Co. KG	Freigabeempfehlung	BAAINBw, Kein	EU
Telefonverschlüsselung	TCU 7000 E 1.1	Elbit Systems Deutschland GmbH & Co. KG	Zulassung	BAAINBw	EU
Telefonverschlüsselung	ELCRODAT 5-4 (V03.10, V03.20, V03.30ctak, V03.40ctak)	Rohde & Schwarz SIT GmbH	Zulassung	DEUmilSAA	EU
Funkgeräte (konventionell und SDR)	Mission Counter Daesh	Motorola Solutions Germany GmbH	Freigabeempfehlung	DEUmilSAA	EU
Funkgeräte (konventionell und SDR)	Teilhabe BOS am StO Büchel	Motorola Solutions Germany GmbH	Freigabeempfehlung	DEUmilSAA	EU
Funkgeräte (konventionell und SDR)	XM6923L_6163.0807.62	Rohde & Schwarz	Zulassung	DEUmilSAA	EU
Funkgeräte (konventionell und SDR)	SVFuA-Grundgerät	Rohde & Schwarz	Zulassung	BAAINBw	EU
E-Mail-und Dateiverschlüsselung	cryptovision GreenShield V1R3	cv cryptovision GmbH	Zulassung	DEUmilSAA	EU
E-Mail-und Dateiverschlüsselung	cv act s/mail 4.0.X	cv cryptovision GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sichere mobile Lösung	MeCrypt 1.7x (BND)	GSMK Gesellschaft für Sichere Mobile Kommunikation mbH	Einsatzerlaubnis	BND	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Sichere mobile Lösung	SecureDOK Government SDS für iOS	Materna Virtual Solution GmbH	Einsatzerlaubnis	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für Android 8.x	Materna Virtual Solution GmbH	Einsatzerlaubnis	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x (AA)	Materna Virtual Solution GmbH	Einsatzerlaubnis	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	INDIGO 15.x	Apple Inc.	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	USA
Sichere mobile Lösung	MeCrypt 1.7x (BND)	GSMK Gesellschaft für Sichere Mobile Kommunikation mbH	Freigabeempfehlung	BND	EU
Sichere mobile Lösung	SecureDOK Government SDS für iOS 8.x	Materna Virtual Solution GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x (iSC)	Materna Virtual Solution GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecuVOICE für iOS und Android 5.x	Secusmart GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	indigo 16.x	Apple Inc.	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	USA

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Sichere mobile Lösung	MECrypt 1.7x	GSMK Gesellschaft für Sichere Mobile Kommunikation mbH	Freigabeempfehlung	BND	EU
Sichere mobile Lösung	SecureDOK Government SDS für iOS 8.x	Materna Virtual Solution GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS (iSC)	Materna Virtual Solution GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	Wire Bund_3.x	Wire Swiss GmbH	Freigabeempfehlung	BKAmt	EU
Sichere mobile Lösung	Wire Bund 3.x	Wire Swiss GmbH	Freigabeempfehlung	BKAmt	EU
Sichere mobile Lösung	SecurePIM Government SDS für Android 7.x	Materna Virtual Solution GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x (AA)	Materna Virtual Solution GmbH	Freigabeempfehlung	Auswärtiges Amt	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x (AA)	Materna Virtual Solution GmbH	Freigabeempfehlung	Auswärtiges Amt	EU
Sichere mobile Lösung	SecuSUITE for Samsung Knox 1.16.0	Secusmart GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sichere mobile Lösung	SecuSUITE for Samsung Knox 1.17.x	Secusmart GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x (NATO)	Materna Virtual Solution GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x	Materna Virtual Solution GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x	Materna Virtual Solution GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x	Materna Virtual Solution GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Client	genuconnect 1.4 Szenario VS-NfD Software-VPN	genua GmbH	Freigabeempfehlung	DEUmilSAA	EU
VPN-Client	genuconnect 1.3	genua GmbH	Zulassung	DEUmilSAA	EU
VPN-Client	genuconnect 2.0	genua GmbH	Zulassung	DEUmilSAA	EU
VPN-Client	NCP VS GovNet Connector 2.X	NCP engineering GmbH	Zulassung	BMG	EU
VS-Arbeitsplatz	SINA Communicator H 1.0 (Geräteklasse für Feldtest R-VSK)	secunet Security Networks AG	Freigabeempfehlung	Auswärtiges Amt	EU
VS-Arbeitsplatz	R&S®Trusted Endpoint Suite (TES) 1.x	Rohde & Schwarz Cybersecurity GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation S/SINA L3 Box S	secunet Security Networks AG	Zulassung	BND	EU
VS-Arbeitsplatz	SINA Terminal E 2.8	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Terminal H 2.8 (Geräteklassen DEU-0101 und DEU-1101)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
VS-Arbeitsplatz	SINA Workstation E 3.6	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Terminal E 3.6 (Wyse-Client)	secunet Security Networks AG	Zulassung	LfV Sachsen, LfV Sachsen-Anhalt	EU
VS-Arbeitsplatz	SINA Workstation E 2.8	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation S 3.5	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Terminal E 3.6	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation E 3.6.x	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation H 3.6 (Geräteklasse DEU-0101 und DEU-1101)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation H 2.8 (Geräteklassen DEU-0101 und DEU-1101)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation H 3.6.x	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	M4Com Crypto-Device (MCD-2-1/1)	M4Com System GmbH	Freigabeempfehlung	DEUmilSAA	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
VPN-Gateway	VeRA_1.0	IT Baden-Württemberg	Freigabeempfehlung	Innenministerium BW	EU
VPN-Gateway	NCP VS GovNetServer 2.x	NCP engineering GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	SDoT Security Gateway Express 1.1	INFODAS GmbH	Zulassung	DEUmilSAA	EU
VPN-Gateway	genuscreen/genucard 7.2	genua GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik), Kein	EU
VPN-Gateway	SDoT Security Gateway Express 1.0	INFODAS GmbH	Zulassung	DEUmilSAA	EU
VPN-Gateway	NCP Secure VPN GovNetServer	NCP engineering GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	SINA L3 Box E 3.10	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	SINA L3 Box S 3.7	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	SINA L3 Box S 3.9	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	SINA L3 Box H 3.10 (Geräteklassen DEU-0101 und DEU-1101)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Verschlüsselung Layer 1	9TCE-PCN-10GU+AES10G-G 211.x.y	Adva Network Security GmbH	Zulassung	LKA Bayern	EU
Verschlüsselung Layer 1	10TCE-PCN-16GU+AES100G-BSI 211.x.y	Adva Network Security GmbH	Zulassung	LKA Bayern	EU
Verschlüsselung Layer 1	10TCE-PCN-16GU+AES100G-BSI 211.x.y (VS-V)	Adva Network Security GmbH	Zulassung	VBL	EU
Verschlüsselung Layer 2	R&S®SITLineETH NG	Rohde & Schwarz Cybersecurity GmbH	Zulassung	DEUmilSAA	EU
Verschlüsselung Layer 2	SINA L2 Box S 3.3.4 (Portfolio)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Verschlüsselung Layer 2	SINA L2 Box S 3.4 (Portfolio)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Verschlüsselung Layer 2	SINA L2 Box H 1.0.x	secunet Security Networks AG	Zulassung	BND, DEUmilSAA	EU
Verschlüsselung Layer 2	atmedia Link Encryptor 3.3.3	atmedia GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Verschlüsselung Layer 2	atmedia Link Encryptor 3.3.4	atmedia GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Verschlüsselung Layer 2	SINA L2 Box S 3.3.2, 3.3.3	secunet Security Networks AG	Zulassung	BKA	EU
Verschlüsselung Layer 2	atmedia LInk Encryptor	atmedia GmbH	Zulassung	BKA	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Verschlüsselung Layer 3	OpenVPN (Notversorgung COVID-19)	OpenVPN Technologies, Inc	Freigabeempfehlung	DEUmilSAA	USA
HSM/Kryptobeschleuniger	CryptoServer 5.2.0.0 (BVA)	Utimaco IS GmbH	Freigabeempfehlung	BVA	EU
HSM/Kryptobeschleuniger	CryptoServer CP5 VS-NfD (VS-V Bdr)	Utimaco IS GmbH	Freigabeempfehlung	Bundesdruckerei	EU
HSM/Kryptobeschleuniger	CryptoServer_5.1	Utimaco IS GmbH	Zulassung	BVA, ITZBund	EU
Sonstiges	SNS Infrastruktur 3.x	Secusmart GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sonstiges	SNS Infrastruktur 1.0 (NdB)	Secusmart GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sonstiges	Secure Tactical Core System 1.0 (DEUmilSAA)	blackned GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sonstiges	Secure Tactical Core System 1.0 (DEUmilSAA)	blackned GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sonstiges	Secure Tactical Core System 1.0 (DEUmilSAA)	blackned GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sonstiges	Secure Tactical Core System 1.0 (DEUmilSAA)	blackned GmbH	Freigabeempfehlung	DEUmilSAA	EU
VS-Registratursysteme	SINA Workflow (SWF) 4.3.x	secunet Security Networks AG	Zulassung	Auswärtiges Amt	EU
Firewall	secunetSBC 6.1	secunet Security Networks AG	Freigabeempfehlung	BDBOS	EU
Firewall	genuate NdB WebRTC	genua GmbH	Einsatzerlaubnis	genua GmbH	EU
Firewall	secunetSBC 6.1	secunet Security Networks AG	Freigabeempfehlung	BDBOS	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Datendiode	Sina One Way H 1.0	secunet Security Networks AG	Freigabeempfehlung	DEUmilSAA	EU
Datendiode	SDoT Software Data Diode 1.3	INFODAS GmbH	Zulassung	DEUmilSAA	EU
VS-Guard	SECCOM® Secure Exchange Gateway (SEG) 4.2.1.0 (im Umfeld GIADS)	Airbus Defence and Space GmbH	Freigabeempfehlung	DEUmilSAA	EU
VS-Guard	SECCOM® Secure Exchange Gateway (SEG) 4.2.5.1.8.0 (im Umfeld SARah)	Airbus Defence and Space GmbH	Freigabeempfehlung	DEUmilSAA	EU
VS-Guard	SEG 4.2.5.1 (Anpassentwicklung ATTS (Ausbildungs- Trainings- und Testsystem) GIADS /KOFA)	Airbus Defence and Space GmbH	Freigabeempfehlung	DEUmilSAA	EU
VS-Guard	SDoT Security Gateway 6.1 Patch1	INFODAS GmbH	Einzelzulassung	DEUmilSAA	EU
VS-Guard	SECCOM® Secure Exchange Gateway (SEG) 5.x	Airbus Defence and Space GmbH	Zulassung	DEUmilSAA	EU
Hypervisor	SecuStack 21.06 (in der Ausprägung "SecuStack Titan“)	secunet Security Networks AG	Zulassung	Auswärtiges Amt	EU
Mobile Device Management, Sichere mobile Lösung	IdZ ES CHARON (Infanterist der Zukunft, Erweitertes System) 2.X (VJTF)	Rheinmetall Defence Electronic GmbH	Zulassung	DEUmilSAA	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Schlüsselspeicher-und Verteilkomponente	ED7-FN oSMS	Rohde & Schwarz SIT GmbH	Freigabeempfehlung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	ED7 oSMS für ED7-FN mit CApp SCIP	Rohde & Schwarz SIT GmbH	Freigabeempfehlung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	BBKME II	Thales Deutschland GmbH	Zulassung	BMVI	EU
Schlüsselspeicher-und Verteilkomponente	Keyserver 8.0	genua GmbH	Zulassung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	KPE III	Thales Deutschland GmbH	Zulassung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	"SMS SVFuA"	Rohde & Schwarz GmbH & Co. KG	Zulassung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	CCMU	Thales Deutschland GmbH	Zulassung	DEUmilSAA	EU
Schlüsselspeicher-und Verteilkomponente	DTD II	Thales Deutschland GmbH	Zulassung	DEUmilSAA	EU
Verschlüsselungsgerät für Satellitensysteme	SAR-Lupe Bodensegment	OHB System AG	Zulassung	DEUmilSAA	EU
Verschlüsselungsgerät für Satellitensysteme	H2Sat-GCU	OHB System AG	Zulassung	DEUmilSAA	EU
Verschlüsselungsgerät für Satellitensysteme	H2Sat-SSU	OHB System AG	Zulassung	DEUmilSAA	EU
Verschlüsselungsgerät für Satellitensysteme	PROOF mini PRS SM Receiver	Siemens AG	Zulassung	BMVI	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Verschlüsselungsgerät für Satellitensysteme	SARah (Phased Array)	DSI Informationstechnik GmbH	Zulassung	DEUmilSAA	EU
Dateiverschlüsselung (stand-alone)	Chiasmus_Kommandozeile_fuer_die_Bundeswehr	BSI - Bundesamt für Sicherheit in der Informationstechnik	Freigabeempfehlung	DEUmilSAA	EU
Dateiverschlüsselung (stand-alone)	Chiasmus_Linux_fuer_die_Bundeswehr	BSI - Bundesamt für Sicherheit in der Informationstechnik	Freigabeempfehlung	DEUmilSAA	EU
Dateiverschlüsselung (stand-alone)	Chiasmus_Kommandozeile_fuer_die_Bundeswehr	BSI - Bundesamt für Sicherheit in der Informationstechnik	Freigabeempfehlung	DEUmilSAA	EU
Dateiverschlüsselung (stand-alone)	Chiasmus_Linux_fuer_die_Bundeswehr	BSI - Bundesamt für Sicherheit in der Informationstechnik	Freigabeempfehlung	DEUmilSAA	EU
Dateiverschlüsselung (stand-alone)	Chiasmus_fuer_Windows_fuer_die_Schluesselerzeugung_bei_der_Bundeswehr	BSI - Bundesamt für Sicherheit in der Informationstechnik	Freigabeempfehlung	DEUmilSAA	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Festplattenverschlüsselung	SafeGuard Device Encryption	Sophos GmbH	Freigabeempfehlung	DEUmilSAA	EU
Festplattenverschlüsselung	R&S Trusted Storage Module	Rohde & Schwarz Cybersecurity GmbH	Zulassung	BMWK	EU
Festplattenverschlüsselung	R&S®Trusted Disk 3.X (Verwendung im IdZ ES - Führungsrechner, (VJTF) Very High Readiness Joint	Rohde & Schwarz Cybersecurity GmbH	Zulassung	DEUmilSAA	EU
Festplattenverschlüsselung	R&S®Trusted Disk 3.X (Verwendung im IdZ ES-Führungsrechner)	Rohde & Schwarz Cybersecurity GmbH	Zulassung	DEUmilSAA	EU
Festplattenverschlüsselung	Utimaco DiskEncrypt 9_00	Utimaco GmbH	Zulassung	DEUmilSAA	EU
Sicherer mobiler Datenträger	Kobra Drive VS und Kobra Stick VS 1.x	DIGITTRADE GmbH	Zulassung	BMWK	EU
Sicherer mobiler Datenträger	Kobra Drive VS und Kobra Stick VS 1.0	DIGITTRADE GmbH	Zulassung	BMWK	EU
Telefonverschlüsselung	ED7-FN mit CApp SCIP	Rohde & Schwarz SIT GmbH	Freigabeempfehlung	DEUmilSAA	EU
Telefonverschlüsselung	ED7-FN mit CApp SCIP	Rohde & Schwarz SIT GmbH	Freigabeempfehlung	DEUmilSAA	EU
Telefonverschlüsselung	TCU 7000 E 1.0	Elbit Systems Deutschland GmbH & Co. KG	Freigabeempfehlung	BAAINBw, Kein	EU
Telefonverschlüsselung	TCU 7000 E 1.1	Elbit Systems Deutschland GmbH & Co. KG	Zulassung	BAAINBw	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Telefonverschlüsselung	ELCRODAT 5-4 (V03.10, V03.20, V03.30ctak, V03.40ctak)	Rohde & Schwarz SIT GmbH	Zulassung	DEUmilSAA	EU
Funkgeräte (konventionell und SDR)	Mission Counter Daesh	Motorola Solutions Germany GmbH	Freigabeempfehlung	DEUmilSAA	EU
Funkgeräte (konventionell und SDR)	Teilhabe BOS am StO Büchel	Motorola Solutions Germany GmbH	Freigabeempfehlung	DEUmilSAA	EU
Funkgeräte (konventionell und SDR)	XM6923L_6163.0807.62	Rohde & Schwarz	Zulassung	DEUmilSAA	EU
Funkgeräte (konventionell und SDR)	SVFuA-Grundgerät	Rohde & Schwarz	Zulassung	BAAINBw	EU
E-Mail-und Dateiverschlüsselung	cryptovision GreenShield V1R3	cv cryptovision GmbH	Zulassung	DEUmilSAA	EU
E-Mail-und Dateiverschlüsselung	cv act s/mail 4.0.X	cv cryptovision GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sichere mobile Lösung	MeCrypt 1.7x (BND)	GSMK Gesellschaft für Sichere Mobile Kommunikation mbH	Einsatzerlaubnis	BND	EU
Sichere mobile Lösung	SecureDOK Government SDS für iOS	Materna Virtual Solution GmbH	Einsatzerlaubnis	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für Android 8.x	Materna Virtual Solution GmbH	Einsatzerlaubnis	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x (AA)	Materna Virtual Solution GmbH	Einsatzerlaubnis	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	INDIGO 15.x	Apple Inc.	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	USA
Sichere mobile Lösung	MeCrypt 1.7x (BND)	GSMK Gesellschaft für Sichere Mobile Kommunikation mbH	Freigabeempfehlung	BND	EU
Sichere mobile Lösung	SecureDOK Government SDS für iOS 8.x	Materna Virtual Solution GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x (iSC)	Materna Virtual Solution GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecuVOICE für iOS und Android 5.x	Secusmart GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	indigo 16.x	Apple Inc.	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	USA
Sichere mobile Lösung	MECrypt 1.7x	GSMK Gesellschaft für Sichere Mobile Kommunikation mbH	Freigabeempfehlung	BND	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Sichere mobile Lösung	SecureDOK Government SDS für iOS 8.x	Materna Virtual Solution GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS (iSC)	Materna Virtual Solution GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	Wire Bund_3.x	Wire Swiss GmbH	Freigabeempfehlung	BKAmt	EU
Sichere mobile Lösung	Wire Bund 3.x	Wire Swiss GmbH	Freigabeempfehlung	BKAmt	EU
Sichere mobile Lösung	SecurePIM Government SDS für Android 7.x	Materna Virtual Solution GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x (AA)	Materna Virtual Solution GmbH	Freigabeempfehlung	Auswärtiges Amt	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x (AA)	Materna Virtual Solution GmbH	Freigabeempfehlung	Auswärtiges Amt	EU
Sichere mobile Lösung	SecuSUITE for Samsung Knox 1.16.0	Secusmart GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sichere mobile Lösung	SecuSUITE for Samsung Knox 1.17.x	Secusmart GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x (NATO)	Materna Virtual Solution GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x	Materna Virtual Solution GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x	Materna Virtual Solution GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sichere mobile Lösung	SecurePIM Government SDS für iOS 8.x	Materna Virtual Solution GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Client	genuconnect 1.4 Szenario VS-NfD Software-VPN	genua GmbH	Freigabeempfehlung	DEUmilSAA	EU
VPN-Client	genuconnect 1.3	genua GmbH	Zulassung	DEUmilSAA	EU
VPN-Client	genuconnect 2.0	genua GmbH	Zulassung	DEUmilSAA	EU
VPN-Client	NCP VS GovNet Connector 2.X	NCP engineering GmbH	Zulassung	BMG	EU
VS-Arbeitsplatz	SINA Communicator H 1.0 (Geräteklasse für Feldtest R-VSK)	secunet Security Networks AG	Freigabeempfehlung	Auswärtiges Amt	EU
VS-Arbeitsplatz	R&S®Trusted Endpoint Suite (TES) 1.x	Rohde & Schwarz Cybersecurity GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation S/SINA L3 Box S	secunet Security Networks AG	Zulassung	BND	EU
VS-Arbeitsplatz	SINA Terminal E 2.8	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Terminal H 2.8 (Geräteklassen DEU-0101 und DEU-1101)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation E 3.6	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
VS-Arbeitsplatz	SINA Terminal E 3.6 (Wyse-Client)	secunet Security Networks AG	Zulassung	LfV Sachsen, LfV Sachsen-Anhalt	EU
VS-Arbeitsplatz	SINA Workstation E 2.8	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation S 3.5	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Terminal E 3.6	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation E 3.6.x	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation H 3.6 (Geräteklasse DEU-0101 und DEU-1101)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation H 2.8 (Geräteklassen DEU-0101 und DEU-1101)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VS-Arbeitsplatz	SINA Workstation H 3.6.x	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	SINA Box M 2.0	secunet Security Networks AG	Zulassung	BfV	EU
VPN-Gateway	M4Com Crypto-Device (MCD-2-1/1)	M4Com System GmbH	Freigabeempfehlung	DEUmilSAA	EU
VPN-Gateway	VeRA_1.0	IT Baden-Württemberg	Freigabeempfehlung	Innenministerium BW	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
VPN-Gateway	NCP VS GovNetServer 2.x	NCP engineering GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	SDoT Security Gateway Express 1.1	INFODAS GmbH	Zulassung	DEUmilSAA	EU
VPN-Gateway	genuscreen/genucard 7.2	genua GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik), Kein	EU
VPN-Gateway	SDoT Security Gateway Express 1.0	INFODAS GmbH	Zulassung	DEUmilSAA	EU
VPN-Gateway	NCP Secure VPN GovNetServer	NCP engineering GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	SINA L3 Box E 3.10	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	SINA L3 Box M 3 SW-Version 2.2 (zur Verschlüsselung von Verbindungen in Nicht-NATO Staaten)	secunet Security Networks AG	Zulassung	BND	EU
VPN-Gateway	SINA L3 Box S 3.7	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
VPN-Gateway	SINA L3 Box S 3.9	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
VPN-Gateway	SINA L3 Box H 3.10 (Geräteklassen DEU-0101 und DEU-1101)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Verschlüsselung Layer 1	9TCE-PCN-10GU+AES10G-G 211.x.y	Adva Network Security GmbH	Zulassung	LKA Bayern	EU
Verschlüsselung Layer 1	10TCE-PCN-16GU+AES100G-BSI 211.x.y	Adva Network Security GmbH	Zulassung	LKA Bayern	EU
Verschlüsselung Layer 1	10TCE-PCN-16GU+AES100G-BSI 211.x.y (VS-V)	Adva Network Security GmbH	Zulassung	VBL	EU
Verschlüsselung Layer 2	R&S®SITLineETH NG	Rohde & Schwarz Cybersecurity GmbH	Zulassung	DEUmilSAA	EU
Verschlüsselung Layer 2	SINA L2 Box S 3.3.4 (Portfolio)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Verschlüsselung Layer 2	SINA L2 Box S 3.4 (Portfolio)	secunet Security Networks AG	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Verschlüsselung Layer 2	SINA L2 Box H 1.0.x	secunet Security Networks AG	Zulassung	BND, DEUmilSAA	EU
Verschlüsselung Layer 2	atmedia Link Encryptor 3.3.3	atmedia GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Verschlüsselung Layer 2	atmedia Link Encryptor 3.3.4	atmedia GmbH	Zulassung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU

Produkttyp	Name	Hersteller	Art	Antragsteller	Hauptsitz des Herstellers
Verschlüsselung Layer 2	SINA L2 Box S 3.3.2, 3.3.3	secunet Security Networks AG	Zulassung	BKA	EU
Verschlüsselung Layer 2	atmedia LInk Encryptor	atmedia GmbH	Zulassung	BKA	EU
Verschlüsselung Layer 3	OpenVPN (Notversorgung COVID-19)	OpenVPN Technologies, Inc	Freigabeempfehlung	DEUmilSAA	USA
HSM/Kryptobeschleuniger	CryptoServer 5.2.0.0 (BVA)	Utimaco IS GmbH	Freigabeempfehlung	BVA	EU
HSM/Kryptobeschleuniger	CryptoServer CP5 VS-NfD (VS-V Bdr)	Utimaco IS GmbH	Freigabeempfehlung	Bundesdruckerei	EU
HSM/Kryptobeschleuniger	CryptoServer_5.1	Utimaco IS GmbH	Zulassung	BVA, ITZBund	EU
Sonstiges	SNS Infrastruktur 3.x	Secusmart GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sonstiges	SNS Infrastruktur 1.0 (NdB)	Secusmart GmbH	Freigabeempfehlung	BSI (Bundesamt für Sicherheit in der Informationstechnik)	EU
Sonstiges	Secure Tactical Core System 1.0 (DEUmilSAA)	blackned GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sonstiges	Secure Tactical Core System 1.0 (DEUmilSAA)	blackned GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sonstiges	Secure Tactical Core System 1.0 (DEUmilSAA)	blackned GmbH	Freigabeempfehlung	DEUmilSAA	EU
Sonstiges	Secure Tactical Core System 1.0 (DEUmilSAA)	blackned GmbH	Freigabeempfehlung	DEUmilSAA	EU
VS-Registratursysteme	SINA Workflow (SWF) 4.3.x	secunet Security Networks AG	Zulassung	Auswärtiges Amt	EU

Anlage 3 zur Antwort auf Frage 13 der Kleinen Anfrage 20/8103

Name	Hersteller	Verhandlungsverfahren
Sina One Way H 1.0	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
secunetSBC 6.1	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
secunetSBC 6.1	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
ED7-FN mit CApp SCIP	Rohde & Schwarz SIT GmbH	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im November 2022
SINA L2 Box S 3.3.4 (Portfolio)	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA L2 Box S 3.4 (Portfolio)	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA L2 Box H 1.0.x	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA L2 Box S 3.3.2, 3.3.3	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA L3 Box E 3.10	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA L3 Box S 3.7	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA L3 Box S 3.9	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA L3 Box H 3.10 (Geräteklassen DEU-0101 und DEU-1101)	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Communicator H 1.0 (Geräteklasse für Feldtest R-VSK)	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Workstation S/SINA L3 Box S	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Terminal E 2.8	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Terminal H 2.8 (Geräteklassen DEU-0101 und DEU-1101)	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022

Name	Hersteller	Verhandlungsverfahren
SINA Workstation E 3.6	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Workstation E 2.8	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Workstation S 3.5	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Terminal E 3.6	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Workstation E 3.6.x	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Workstation H 3.6 (Geräteklasse DEU-0101 und DEU-1101)	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Workstation H 2.8 (Geräteklassen DEU-0101 und DEU-1101)	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Workstation H 3.6.x	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA Workflow (SWF) 4.3.x	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
Sina One Way H 1.0	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
secunetSBC 6.1	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
secunetSBC 6.1	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
ED7-FN mit CApp SCIP	Rohde & Schwarz SIT GmbH	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im November 2022
SINA L2 Box S 3.3.4 (Portfolio)	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA L2 Box S 3.4 (Portfolio)	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022

Name	Hersteller	Verhandlungsverfahren
SINA L2 Box H 1.0.x	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022
SINA L2 Box S 3.3.2, 3.3.3	secunet Security Networks AG	Verhandlungsverfahren ohne TNW nach VSVgV mit Hersteller des Produkts im April 2022