Befragung der Parteien im Vorfeld der Bundestagswahl 2017 zum Thema „IT-Sicherheit“

Die NIFIS Nationale Initiative für Informations- und Internet-Sicherheit e.V., eine neutrale Selbsthilfeorganisation, die die deutsche Wirtschaft im Kampf gegen die täglich wachsenden Bedrohungen aus dem Netz technisch, organisatorisch und rechtlich unterstützen möchte,
hat im Vorfeld der Bundestagswahl 2017 Parteien zum Thema „IT-Sicherheit“ befragt.

Es kamen sowohl aktuelle Fragen der IT-Sicherheit zur Sprache, als auch die Frage nach den jeweiligen Maßnahmen, die die einzelnen Parteien ergreifen möchten. Befragt wurden alle Parteien, die seit der Wahl zum ersten Bundestag im Jahr 1949 die 5 Prozent Hürde genommen haben: Bündnis 90/Die Grünen, CDU / CSU, Die LINKE, FDP, SPD.

Im Einzelnen haben geantwortet:

Bündnis 90/Die Grünen:
Dr. Konstantin von Notz, MdB, Stellv. Fraktionsvorsitzender und Sprecher für Netzpolitik

CDU / CSU:
Thomas Jarzombek, MdB, Mitglied der Enquete-Kommission "Internet und digitale Gesellschaft“; Mitglied im Unterausschuss "Neue Medien", Beirat der NIFIS

Fraktion DIE LINKE:
Jan Korte, MdB, Stellvertretender Fraktionsvorsitzender, Fraktion DIE LINKE

FDP:
Nicola Beer, MdB, Generalsekretärin und Manuel Höferlin, MdB, ehemaliger Beirat der NIFIS

SPD
Lars Klingbeil, MdB, Netzpolitischer Sprecher der SPD-Bundestagsfraktion, Vorsitzender der Landesgruppen Niedersachsen/Bremen in der SPD-Bundestagsfraktion SPD

Aufgrund unserer Neutralität wurden die Antworten im Folgenden in alphabetischer Reihenfolge aufgelistet und in voller Gänze wiedergegeben.

Frage 1:

Wie wichtig stufen Sie die Bedeutung der IT-Sicherheit ein?

a) für die Politik
b) für die Wirtschaft
c) für die Bürger

Bündnis 90/Die Grünen:
IT-Sicherheit hat für alle drei eine außerordentlich hohe Bedeutung erlangt. Für die Politik waren die Snowden-Leaks sowie der Bundestags-Hack ein Weckruf. Für die Wirtschaft ganz besonders die geheimdienstlichen Verwicklungen von NSA, BND usw., welche klare Hinweise auf Industrie- und Wirtschaftsspionage nicht bloß von den üblichen Verdächtigen China und Russland erbrachten, sondern von den westlichen Geheimdiensten selbst. Deutlich wird: Die Daten der Bürgerinnen und Bürger sind weder bei Verwaltung noch Wirtschaft in sicheren Händen.

CDU / CSU:
CDU und CSU stehen für eine umfassende IT-Sicherheit. Die Widerstandsfähigkeit der deutschen Wirtschaft wird tagtäglich auf die Probe gestellt. Deutsche Unternehmen und ihre Mitarbeiter sind weltweit angesichts fortschreitender Globalisierung und zunehmender Vernetzung vielfältigen Bedrohungen ausgesetzt. Diese reichen von Cyberattacken, Wirtschaftsspionage und -kriminalität bis hin zu Sabotage.
Durch Forschung und Entwicklung entstehen jeden Tag neue und sichere Arbeitsplätze in Deutschland. Vor allem die innovativen Produkte der deutschen Wirtschaft stehen seit Jahren im Visier ausländischer Konkurrenten und Nachrichtendienste. Knowhow und Innovationsfähigkeit sind Schlüsselfaktoren der Wettbewerbsfähigkeit deutscher Unternehmen.

Die Angriffe erfolgen konventionell und digital – häufig auch kombiniert. Eine wirksame Abwehr gegen diese vielschichtigen Sicherheitsrisiken für die deutschen Unternehmen können weder die Unternehmen noch die Sicherheitsbehörden alleine leisten. Insbesondere kleine und mittelständische Unternehmen sind häufig nur unzureichend gegen Spähangriffe geschützt. Unternehmen müssen daher noch intensiver für IT-Sicherheitsfragen sensibilisiert und darüber aufgeklärt werden, wie sie sich bestmöglich schützen können.

Mit dem IT-Sicherheitsgesetz wurde ein einheitlicher Mindeststandard für Betreiber kritischer Infrastrukturen, Betreiber von Web-Angeboten und Telekommunikationsunternehmen in Deutschland geschaffen, verbunden mit Meldepflichten bei kritischen Vorfällen. Ziel ist die Verbesserung der IT-Sicherheit bei Unternehmen und in der Bundesverwaltung, sowie ein besserer Schutz der Bürgerinnen und Bürger im Internet.

Die LINKE:
Hier kann es aus unserer Sicht keine Abstufung geben. IT-Sicherheit hat aus unterschiedlichen Gründen für die genannten Gruppen eine hohe Bedeutung, da wesentliche Teile den politischen, wirtschaftlichen und privaten Lebens ohne eine sichere und integre IT nicht mehr zu bewerkstelligen sind.

FDP:

a) Sehr wichtig.
b) Sehr wichtig.
c) Sehr wichtig.

Die zunehmende Vernetzung und Digitalisierung der Welt bietet uns einzigartige Chancen. Digitale Technologien ermöglichen viele neue Produkte und Dienstleistungen (zum Beispiel selbstfahrende Autos, vollständig neue Lieferservices etwa mit Drohnen, ferngesteuerte chirurgische Eingriffe etc.). Gleichzeitig stellt uns die IT-Sicherheit vor große Herausforderungen, wie beispielsweise Missbrauchs- und Gefahrenpotenzial vorzubeugen. Wir Freie Demokraten setzen uns daher für eine Verbesserung der nationalen und europäischen Strategie zur Cybersicherheit (Cyber-Security) ein.

SPD:
a) für die Politik
Sehr wichtig.
b) für die Wirtschaft
Sehr wichtig.
c) für die Bürger
Sehr wichtig. IT-Sicherheit kommt in allen Bereichen eine grundlegende Bedeutung zu. IT-Sicherheit ist eine der zentralen Voraussetzungen für den Erfolg der Digitalisierung.

Frage 2:

Stimmen Sie folgenden Aussagen zu?

a) IT-Sicherheit gehört zu den größten Herausforderungen der nächsten Jahre
b) Die Gewährleistung der IT-Sicherheit ist in erster Linie eine staatliche Aufgabe
c) Die Wirtschaft muss ich in erster Linie selbst gegen Cyberangriffe schützen
d) Die Bürger haben persönlich Sorge für die IT-Sicherheit zu tragen

Bündnis 90/Die Grünen:
a) „IT-Sicherheit gehört zu den größten Herausforderungen der nächsten Jahre“ trifft es am besten. Verantwortlich sind alle zusammen, in enger Kooperation und aufgrund klarer gesetzlicher Regelungen. Selbstschutz allein trägt weder bei den Bürgern noch in der Wirtschaft den Risiken angemessen Rechnung.

CDU / CSU:
2a. „IT-Sicherheit gehört zu den größten Herausforderungen der nächsten Jahre“ Ja.
2b. „Die Gewährleistung der IT-Sicherheit ist in erster Linie eine staatliche Aufgabe“ Nein. Weder der Staat, noch die Bürger oder Unternehmen können IT-Sicherheit alleine sicherstellen.
2c. „Die Wirtschaft muss ich in erster Linie selbst gegen Cyberangriffe schützen“ Nein. Weder der Staat, noch die Bürger oder Unternehmen können IT-Sicherheit alleine sicherstellen.
2d. „Die Bürger haben persönlich Sorge für die IT-Sicherheit zu tragen“ Wir wollen nicht, dass Mängel bei der Sicherheit von IT-Produkten bei den Kunden zu vermeidbaren Schäden führen. Dennoch bleibt natürlich deren Verantwortung für die IT-Sicherheit (Updates ausführen, Virenschutzprogramme usw.) bestehen.

Die LINKE:

a) „IT-Sicherheit gehört zu den größten Herausforderungen der nächsten Jahre“ Ja. Dazu zählen für uns auch Vorschriften zur Härtung von IT-Systemen durch die Implementierung einer IT-Produkthaftung.

b) „Die Gewährleistung der IT-Sicherheit ist in erster Linie eine staatliche Aufgabe“ Ja

c) „Die Wirtschaft muss ich in erster Linie selbst gegen Cyberangriffe schützen“ Mit Einschränkungen ja. Allerdings braucht es dafür einen klaren rechtlichen Rahmen, der die Verantwortlichkeit der
Unternehmen und ihre Kooperation mit zuständigen staatlichen Stellen regelt.

d) „Die Bürger haben persönlich Sorge für die IT-Sicherheit zu tragen“ Ja. IT-Sicherheit kann nur funktionieren, wenn alle sich nach ihren Möglichkeiten beteiligen, Bedrohungen einzudämmen.

FDP:

a) „IT-Sicherheit gehört zu den größten Herausforderungen der nächsten Jahre“ Ja.

b) „Die Gewährleistung der IT-Sicherheit ist in erster Linie eine staatliche Aufgabe“ Eher ja. Der effektive Schutz digitaler Netze und Systeme ist staatliche Aufgabe ersten Ranges. In enger Zusammenarbeit mit den hier aktiven Unternehmen, mit Wissenschaft und mit IT-Experten wollen wir deshalb die Cybersicherheit stärken und weiterentwickeln.

c) „Die Wirtschaft muss ich in erster Linie selbst gegen Cyberangriffe schützen“ Neutral.Der Staat muss für sichere Infrastrukturen sorgen, auf deren Basis Unternehmen auch selbst Verantwortung dafür tragen, ihr eigenes Netz, ihre Maschinen etc. angemessen gegen Cyberangriffe zu schützen, unter anderem durch regelmäßige Sicherheitsupdates und sichere Identifikationsverfahren.

d) „Die Bürger haben persönlich Sorge für die IT-Sicherheit zu tragen“ Neutral. Auch die Bürgerinnen und Bürger müssen als Nutzerinnen und Nutzer von digitalen Infrastrukturen und Produkten für die IT-Sicherheit Sorge tragen, indem sie zum Beispiel vom Hersteller empfohlene Prozesse zum Einspielen von Updates befolgen.

SPD:

a) „IT-Sicherheit gehört zu den größten Herausforderungen der nächsten Jahre
Stimme zu.

b) „Die Gewährleistung der IT-Sicherheit ist in erster Linie eine staatliche Aufgabe“
Die Gewährleistung der IT-Sicherheit ist auch eine staatliche Aufgabe, aber nicht allein.

c) „Die Wirtschaft muss ich in erster Linie selbst gegen Cyberangriffe schützen“
Stimme nicht zu. Politik und Wirtschaft müssen gemeinsam IT-Sicherheit sicherstellen. Staat und Wirtschaft sind gemeinsam in der Pflicht, diese Angriffe auf unsere digitalen Infrastrukturen, auf Daten und IT-Systeme wirksam abzuwehren und zu bekämpfen.

d) „Die Bürger haben persönlich Sorge für die IT-Sicherheit zu tragen“
Natürlich müssen auch die Bürgerinnen und Bürger persönlich Sorge für die IT-Sicherheit tragen, sie müssen aber auch in der Lage sein, dies tun zu können. Deswegen wollen wir das IT-Sicherheitsgesetz fortschreiben und weiterentwickeln. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) soll ausgebaut und in seiner neutralen Rolle und Beratungsfunktion gestärkt werden. Das BSI soll für Bürger, Unternehmen und Behörden zum vertrauenswürdigen Dienstleister werden, indem es sichere Hard- und Software zertifiziert sowie über Cyberangriffe und digitale Sicherheitsrisiken informiert. Wir setzen uns darüber für eine eindeutige und faire Haftungskette auch für digitale Produkte und Dienstleistungen ein.

Frage 3:

Cyberkriminalität ist zunehmend ein internationales Phänomen. Täter und Opfer sitzen selten im gleichen Land. Eine Strafverfolgung bei ausländischen Tätern im Ausland stößt jedoch immer wieder auf das Problem, dass die notwendigen Beweise aufwändig oder gar nicht über entsprechende Rechtshilfeersuchen erlangt werden können. Was wollen Sie unternehmen um hier eine schnellere, effizientere Strafverfolgung ausländischer Straftäter zu ermöglichen?

Bündnis 90/Die Grünen
Wir unterstützen die aktuellen Bemühungen um eine rechtsstaatlich wie grundrechtlich angemessene Regelung auf EU-Ebene. Bei Cyberkriminalität wird die Bedeutung der Cybercrime-Konvention unterschätzt, welche bereits wichtige Fortschritte erbracht hat. Die Strafverfolgung ist im Sortiment der Cybersicherheit eine notwendige, aber sicherlich nicht die vordringlichste und absehbar nicht effektivste Form des Umgangs mit Cyberkriminalität. Resilienz steht für uns im Vordergrund.

CDU / CSU:
Deutschland ist als Industriestandort mit einem starken Mittelstand besonders stark davon betroffen, dass immer mehr Prozesse und Produktionsschritte digitalisiert werden und daraus neue potentielle Angriffsziele für Kriminelle entstehen.
Wir wollen die Vorgaben für eine angemessene Verteilung von Verantwortlichkeiten und Sicherheitsrisiken zum Beispiel durch Produkthaftungsregeln für IT-Sicherheitsmängel und Sicherheitsvorgaben für Hard-und Softwarehersteller überprüfen. Wir brauchen eine stärkere Verantwortung der Hersteller, einwandfreie Software zu programmieren und kritische Sicherheitslücken schnell zu stopfen.
Wir wollen nicht, dass Mängel bei der IT-Sicherheit bei den Kunden zu vermeidbaren Schäden führen, wobei natürlich deren Verantwortungsteil für die IT-Sicherheit (Updates ausführen, Virenschutzprogramme usw.) bestehen bleibt.

Die LINKE:
Die zahlreichen bestehenden Abkommen zur Rechtshilfe in Strafsachen müssen den neuen Gegebenheiten angepasst werden, insbesondere bei den bestehenden Regelungen auf Ebene der EU ist dabei auf eine strikt rechtsstaatliche Ausgestaltung zu achten. Allerdings werden wir damit leben müssen, dass sich Straftäter über die Nutzung von Infrastruktur in nicht kooperationswilligen oder –fähigen Staaten einer effizienten Strafverfolgung entziehen.

FDP:
Wir Freie Demokraten wollen eine Verbesserung der nationalen und europäischen Strategie zur Cybersicherheit (Cyber-Security). Die fortschreitende Digitalisierung erhöht zunehmend die Bedeutung des Cyberraums für globale Kommunikation, wirtschaftliche Innovation und strategische Infrastruktureinrichtungen. Ebenso steigt die Relevanz des Cyberraums für Nachrichtendienste und ausländische Streitkräfte sowie Wirtschaftsspionage und organisierte Kriminalität. Allein die deutsche Bundesregierung registriert pro Tag rund 20 hochspezialisierte Cyberangriffe auf die Netze des Bundes. Die Zahl der Cyberangriffe auf große deutsche Unternehmen liegt noch viel höher, wie die rund vier Millionen automatisierten Angriffe pro Tag auf die Infrastruktur der Deutschen Telekom verdeutlichen. Deshalb braucht es sowohl auf nationaler als auch auf europäischer Ebene eine abgestimmte Strategie zum Schutz von privaten Unternehmen und öffentlichen Einrichtungen gleichermaßen, um diesen neuen Bedrohungen zu begegnen. Wir Freie Demokraten wollen das Bundesamt für Sicherheit in der Informationstechnik (BSI) aus der Zuständigkeit des Bundesinnenministeriums lösen und als nachgeordnete Behörde der Fachaufsicht des neu zu schaffenden Digital- und Innovationsministeriums

unterstellen. Nationale Lösungen können aber langfristig alleine nicht bestehen. Auch im Cyberraum lohnt es sich, die europäischen Fähigkeiten zu bündeln. Im globalen Kontext wollen wir den Abschluss eines internationalen Informationsfreiheitsabkommens vorantreiben, das die Freiheit und Unabhängigkeit des Internets auch in Zukunft sichern sowie die Überwachung und Zensur des Internets eindämmen soll.

SPD:
Es gibt bereits heute zahlreiche Vereinbarungen auf europäischer wie auch auf internationaler Ebene, um die Strafverfolgung bei Cyberkriminalität sicherzustellen. Wir müssen vor allem die Strafverfolgungsbehörden besser aufstellen und personell und technisch so ausstatten, dass eine schnelle und effektive Strafverfolgung sichergestellt werden kann.

Frage 4:

Das neue Datenschutzgesetz sowie die EU Grundverordnung sehen zum Teil sehr hohe Bußgelder vor. Dies auch schon für den Bereich der Nichteinhaltung der gesetzlichen Regelungen (und eben nicht erst bei Vorfällen). Jedoch gibt es keine geeigneten Maßnahmen zur Überwachung der Einhaltung der gesetzlichen Vorgaben. Die Landesdatenschutz-beauftragten sind personell unterbesetzt. Welche Maßnahmen wollen Sie einleiten um dies zu verbessern?

Bündnis 90/Die Grünen:
Das Vollzugsdefizit des Datenschutzes kann und muss sich verändern. Die EU-Datenschutzgrundverordnung wird dazu hoffentlich einen Beitrag leisten. Die Aussicht auf Sanktionen allein kann das nicht erreichen. Letztlich muss es einen Bewusstseinswandel in der Wirtschaft geben. Datenschutz muss als Vertrauensanker und als Wettbewerbsvorteil erkannt werden. Dazu zählen auch Instrumente wie Gütesiegel, für die wir uns weiter stark machen. Die Ressourcen der Landesdatenschutzbeauftragten sind Ländersache. Wo wir können, dringen wir auf entsprechend bessere Ausstattung. Auch bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kann und muss es damit weitergehen.

CDU / CSU:
Die Metapher von Daten als Rohstoff und als Öl des 21. Jahrhunderts wird oft benutzt. Das stimmt: Die digitale Ökonomie funktioniert eben genau durch die Verarbeitung von Daten. Deswegen ist es auch wichtig gewesen, hier mit der Datenschutzgrundverordnung einheitliche europäische Regelungen zu schaffen. Die Angleichung unseres nationalen Datenschutzrechts an die europarechtlichen Vorgaben der Datenschutz-Grundverordnung sorgt für die Vereinheitlichung des Datenschutzes im EU-Binnenmarkt. Zugleich reagiert sie auf die Herausforderungen, vor die die fortschreitende Digitalisierung auch den Datenschutz stellt. Um das Ziel der EU-weiten Harmonisierung nicht zu gefährden, haben wir die zahlreichen Öffnungsklauseln, die die Datenschutzgrundverordnung für den nicht-öffentlichen Bereich bereithält, mit Augenmaß gestaltet. Die Nutzung dieser Spielräume wurde zugunsten der Betroffenen und der privaten Wirtschaft mit ihren etablierten Geschäftsmodellen vorgenommen.

Durch die Digitalisierung fallen in großem Maßstab Daten an, deren Verarbeitung zu mehr Wertschöpfung beitragen kann: Daten sind der Rohstoff der Zukunft. Mit der

Datenschutzgrundverordnung der Europäischen Union eröffnet sich der deutschen und europäischen Wirtschaft – ob kleine und mittlere Unternehmen oder globale Konzerne - ein neuer, einheitlicher Handlungsrahmen für digitale Geschäftsmodelle.

Die Verantwortung für die Ausstattung der Landesdatenschutzbeauftragten liegt ausschließlich bei den Bundesländern. Wir wollen die Balance zwischen Datenschutz und Innovation neu justieren. Dazu gehört ein Sachverständigenrat, der für Datenschutzfragen Vorschläge aus dem Blickwinkel der Innovation erarbeitet und vergleichbares auch auf EU Ebene. Wir wollen, dass die Datenschützer zusätzlich einen Arbeitsschwerpunkt „Dateninnovation“ bekommen, um beide Seiten gleichzeitig zu sehen. Wir wollen die Einführung einer zentralen Anlaufstelle (one-stop-shop) für Unternehmen.

Die LINKE:
Für die personelle Ausstattung der Datenschutzaufsicht in den Ländern sind diese selbst verantwortlich. Wir setzen uns dafür ein, dass sowohl im Bund als auch in den Ländern eine aufgabenadäquate personelle Stärkung vorgenommen wird. Bei Umsetzung unseres Steuerkonzepts erhalten die Länder die hierfür notwendigen finanziellen Spielräume.

FDP:
Die EU-Datenschutzgrundverordnung tritt ab 24. Mai 2018 EU-weit in Kraft. Die Bundesrepublik muss diese Verordnung durch Gesetze wie beispielsweise das deutsche Bundesdatenschutzgesetz umsetzen. Damit für Nutzer bester Datenschutz und Rechtssicherheit besteht, müssen wir die Umsetzung möglichst schnell und mit so wenigen Ausnahmen wie möglich vollziehen. So können auch alle Beteiligten besser planen.

Wir wollen auch den institutionellen Datenschutz stärken und den Rechtsrahmen hierfür zwischen Bund und Ländern angleichen. Die Unabhängigkeit der obersten Datenschutzbehörden wollen wir für eine effektive Kontrolle weiter ausbauen. Daneben sind selbstverständlich die notwendigen finanziellen und personellen Grundlagen zu schaffen, um eine Unabhängigkeit des Datenschutzes auch praktisch zu gewährleisten.

SPD:
Die Datenschutzbehörden müssen so ausgestattet werden, dass sie ihre Aufsichts- und Kontrollpflichten wirksam ausüben können.

Frage 5:

In den letzten Jahren wurden im Informationssicherheitsbereich zunehmend Gesetze erlassen, welche Probleme lösen, die nicht oder nur im geringen Umfang existieren, wie z.B. das DE-Mail Gesetz. Welche Maßnahmen wollen Sie durchführen um im Rahmen des Bürokratieabbaus die Sinnhaftigkeit solcher Gesetze zu prüfen und diese ggf. wieder abzuschaffen?

Bündnis 90/Die Grünen:
Das DE-Mail-Gesetz haben wir von Beginn an abgelehnt, weil Bürgervertrauen nur bei konsequenter Ende-Zu-Ende-Verschlüsselung erreichbar gewesen wäre. Ähnliche Großprojekte wie die eID oder die eGK stehen auf der Kippe. Beide haben noch das Potential für Verbesserungen im Sinne der

Bürgerinnen und Bürger. Sie können nur funktionieren, wenn professioneller gearbeitet und die eigentlich Betroffenen besser einbezogen, beteiligt und gehört werden.

CDU / CSU:
Beim Bürokratieabbau sind wir vorangekommen und haben Wirtschaft und Verbrau-cher in dieser Wahlperiode von Bürokratie entlastet. Der jährliche Bürokratieaufwand der Bürger wurde in dieser Wahlperiode um 8,5 Millionen Stunden reduziert. Seit 2015 gilt die „one-in, one-out"-Regel. Diese Regelung hat sich bewährt und wird weiter fortgesetzt.

Gerade für mittelständische Unternehmen sind überbordende bürokratische Anforderungen eine ernste Erschwernis für ihren wirtschaftlichen Erfolg. Wir brauchen deshalb eine neue Gesetzgebungs- und Verwaltungskultur, bei der die Vermeidung oder Begrenzung neuer Regelungen im Vordergrund steht.
Bei neuen Gesetzesvorhaben soll – soweit vertretbar – auf Kontrolle und Regulierung verzichtet werden, bis eine Notwendigkeit dafür eindeutig nachgewiesen ist. Dabei sind natürlich auch die Möglichkeiten der Selbstregulierung zu beachten.

Die LINKE:
Für eine effektive Prävention gegen Bedrohungen der IT-Sicherheit müssen auch die Unternehmen ihren Verpflichtungen nachkommen, zu ihrer Durchsetzung braucht es auch die entsprechenden Behörden, also Bürokratie. Von vornherein zum Scheitern verurteilte Mammutvorhaben wie DE-Mail haben wir immer abgelehnt.

FDP:
Wir Freie Demokraten wollen die Belastungen der Bürgerinnen und Bürger und Betriebe durch zu viel Regulierung abbauen. Dazu schlagen wir eine zeitliche Begrenzung von Gesetzen, sowie das „One in, two out"-Prinzip vor. Neue Regelungen sollen nur dann verabschiedet werden, wenn zugleich in doppeltem Umfang Folgekosten an anderer Stelle zurückgeführt werden. Außerdem sollen neue Regelungen ein Ablaufdatum erhalten, damit regelmäßig überprüft wird, ob sie sich bewähren.

SPD:
Das DE-Mail-Gesetz hätte einen wichtigen Beitrag zum Aufbau einer sicheren und vertrauenswürdigen Infrastruktur leisten können, wenn man es richtiggemacht hätte. Gerade im IT-Bereich sind die Entwicklungen so dynamisch, dass alle gesetzlichen Regelungen zeitnah evaluiert und ggfs. angepasst werden müssen. Unsere Gesellschaft braucht klare Regeln. Unnötige Reglungen oder Bürokratie hingegen müssen abgeschafft werden.

Frage 6:

Es ist allgemein bekannt, dass vorhandene Daten früher oder später missbraucht werden. Dennoch werden Gesetze erlassen, die umfangreiche Datensammlungen ermöglichen. Wie wollen Sie sicher stellen, dass

a) diese Daten nicht in unbefugte Hände gelangen,
b) diese Daten nicht im Rahmen späterer Gesetzgebungen missbraucht werden
c) die Datensammlung auf das absolut notwendige beschränkt bleibt?

Bündnis 90/Die Grünen:
Wir lehnen fragwürdige Projekte der Datenbevorratung ab. So klagen wir gegen die Vorratsdatenspeicherung. Sie bringt auch keinen Sicherheitsgewinn. Gegen terroristische Bedrohung ist es beispielsweise viel wirksamer, gezielt mit verhältnismäßigen Mitteln einige hundert Personen zu überwachen, die hierfür auch einen hinreichenden Anlass geboten haben, als 80 Millionen Bürgerinnen und Bürger anlasslos mit der Vorratsdatenspeicherung. Die PNR, AZRG, BKA-Reform u.v.a. haben wir im Parlament kritisch begleitet und immer wieder auf die Risiken hingewiesen. Wir fordern die Einhegung der Risiken entsprechender bestehender Datenbanken durch Gesetzgeber und Aufsichtsbehörden.

CDU / CSU:
Durch die Digitalisierung fallen in großem Maßstab Daten an, deren Verarbeitung zu mehr Wertschöpfung beitragen kann: Daten sind der Rohstoff der Zukunft. Mit der EU-Datenschutzgrundverordnung wird ein einheitliches Datenschutzregime für einen gemeinsamen digitalen Binnenmarkt geschaffen. Sie tritt im Mai 2018 in Kraft, notwendige Änderungen am Bundesdatenschutzgesetz hat der Bundestag bereits beschlossen. Zum Schutz personenbezogener Daten sind die Möglichkeiten der Pseudonymisierung und der Verschlüsselung zu nutzen.
Wir sagen aber auch ganz deutlich: Datensparsamkeit kann heute nicht mehr die generelle Verhaltens-Leitlinie sein. Denn ein alleiniger Fokus auf sie reduziert Chancen für neue Produkte, Dienstleistungen und Fortschrittsmöglichkeiten. Gerade vor dem Hintergrund der Wettbewerbsfähigkeit, z. B. im Vergleich zu internationalen Plattformen, die von der Erhebung und der Vernetzung leben und monopolartige Stellungen einnehmen, müssen wir unsere deutsche und europäische Positionierung im internationalen Vergleich stärken und ausbauen.

Die LINKE:
Wir haben alle Gesetze abgelehnt, die eine anlasslose Massenspeicherung von Daten eingeführt haben, wie die TKVorratsdatenspeicherung und die Fluggastdatenspeicherung. Nur höchstmögliche Datensparsamkeit bietet eine Gewähr gegen Missbrauch von Daten oder die später vorgenommen Ausweitung ihrer Nutzung.

FDP:
Die Fragen a) bis c) werden im Zusammenhang beantwortet:

In erheblichem Maß sind es staatliche Stellen selbst, die unsere Sicherheit gefährden. Um in Computer, Smartphones und andere von Bürgerinnen, Bürgern und Unternehmen genutzten technischen Geräte eindringen zu können, müssen staatliche Stellen wissen, wo in welchem System welche Sicherheitslücken bestehen. Statt eigene oder über Dritte beschaffte Erkenntnisse an den betroffenen Hersteller zu melden, damit dieser ein die Sicherheitslücke schließendes Update bereitstellen kann, behalten auch staatliche Stellen ihr Wissen für sich, um selbst ungestört in das System eindringen

können. Dadurch wird in Kauf genommen, dass auch Kriminelle diese Sicherheitslücken weiter nutzen können, obwohl staatliche Stellen deren Beseitigung veranlassen könnten.

Um dies zu vermeiden, lehnen wir Freie Demokraten eine Beschaffung von Informationen durch staatliche Stellen auf Grau- und Schwarzmärkten ebenso strikt ab, wie das bewusste Offenhalten und Nutzen von den staatlichen Stellen bekannten Sicherheitslücken.

SPD:
Ich sehe die immer weitergehenden Datensammlungen in immer neuen Sicherheitsgesetzen mit Sorge, etwa die anlasslose Vorratsdatenspeicherung. Zum einen ist bis heute die Wirksamkeit und Notwendigkeit nicht hinreichend belegt, zum anderen gibt es zahlreiche verfassungsrechtliche und auch europarechtliche Bedenken.
Es muss bei jeder Gesetzgebung technisch und rechtlich genau geprüft und abgewogen werden, ob und inwieweit eine Datenerhebung notwendig, verhältnismäßig und mit dem Datenschutz und den grundgesetzlich garantierten Persönlichkeitsrechten vereinbar ist und inwiefern sie zu einem wirklichen Sicherheitsgewinn beiträgt. Dabei muss auch gesetzlich festgeschrieben werden, für welche Zwecke diese Daten verwendet werden dürfen und dass die IT-Sicherheit gewährleistet werden muss.

Frage 7:

Gibt es Überlegungen, die neuen elektronischen Ausweise auch für „Identity & Access Management“ zu nutzen und insbesondere mit „login-Funktionalitäten“ zu versehen, um gemeinsam mit der Industrie einen pragmatischen, funktionierenden und benutzerfreundlichen Weg zum sicheren Login mit Ausweis zu finden?

Bündnis 90/Die Grünen:
Wir haben die Verbindung von staatlicher Ausweisfunktion und privater Geschäftsfunktion von Anfang kritisch als Vermengung von zu Recht getrennt gehaltenen Bereichen gesehen. Die ja bereits bestehende e-ID-Funktion wurde dann aus zahlreichen weiteren Gründen von der Bundesregierung an die Wand gefahren, nicht zuletzt weil sie kein Geld bereitgestellt hat. Jetzt fehlt es an grundlegender Akzeptanz in Wirtschaft und bei Bürgerinnen und Bürgern. Ohne Klärung möglicher Fortschritte bei dieser Vorfrage machen weitere Überlegungen wenig Sinn.

CDU / CSU:
Durch die Einführung eines digitalen Bürgerportals und eines elektronischen Bürgerkontos werden wir sicherstellen, dass praktisch alle Verwaltungsdienstleistungen deutschlandweit elektronisch verfügbar sind. Egal ob Steuererklärung, Antrag auf Kindergeld, PKW-Zulassung oder Anwohnerparkausweis. Das spart Zeit und Geld und ermöglicht zusätzliche Wertschöpfung.

In der abgelaufenen Wahlperiode hat der Bundestag bereits das Gesetz zur Förderung des elektronischen Identitätsnachweises verabschiedet. Ziele sind der stärkere Einsatz und die einfachere Nutzung der Online-Ausweisfunktion (eID-Funktion) des Personalausweises, u. a. bei der Nutzung elektronischer Behördendienste. Außerdem schafft das Gesetz die Grundlage für eine EU-weite Notifizierung der eID-Funktion als elektronisches Identifizierungsmittel, sodass die eID-Funktion mittelfristig auch bei ausländischen Behörden eingesetzt werden kann.

Die LINKE:
Wir sehen die Einführung bzw. verstärkte Implementierung des „elektronischen Identitätsnachweises“ kritisch. Angesichts von Bestrebungen in der gesamten EU, Möglichkeiten der eindeutigen elektronischen Authentifizierung zu finden, die sowohl von staatlicher Seite als auch etwa im Fernhandel zur Anwendung kommen können, wurde hier womöglich eine teure und am Ende wenig effiziente Insellösung geschaffen. Eine Alternative bestünde unseres Erachtens auf gerät- und plattformunabhängigen, offenen Lösungen. Wie diese aussehen können, muss tatsächlich in Kooperation aller Beteiligten entwickelt werden.

FDP:
Ja. Für uns Freie Demokraten muss jeder am digitalisierten Leben teilhaben können – sicher und unkompliziert. Wir wollen den Personalausweis weiter entwickeln zu einer nutzerfreundlichen und sicheren digitalen Identifizierung. Ob gegenüber Behörden, im Gesundheitswesen, im Austausch mit Banken, Unternehmen oder der Nutzer untereinander – überall soll eine sichere, digital nachweisbare Identifizierung zum Einsatz kommen können. Sie könnte alle anderen Berechtigungskarten und Identitätsnachweise ersetzen. Darüber hinaus muss Verschlüsselungstechnologie gemeinsam mit Unternehmen weiterentwickelt werden.

SPD:

Mit der eID-Funktion wurde die Infrastruktur für eine sichere Identifizierung geschaffen. Voraussetzung, dass sich die eID-Funktion als Standardidentifizierungsmittel etabliert, sind interessante und nutzerfreundliche Anwendungen aus Verwaltung und Wirtschaft.

Frage 8:

IT-Sicherheit wird nicht nur von Cyberkriminellen bedroht. "Bundestrojaner" bzw. staatlich verordnete "Backdoors" können ebenfalls Sicherheitslücken in IT-Systemen verursachen bzw. offenlegen, die dann auch von Kriminellen oder fremden Geheimdiensten genutzt werden können. Wie soll nach Ihrer Ansicht ein sinnvoller Ausgleich zwischen Strafverfolgung, Kriminalitätsprävention und Terrorabwehr einerseits und IT-Sicherheit der Bürger und Unternehmen andererseits sichergestellt werden?

Bündnis 90/Die Grünen:
Wir halten die gesetzliche Regelung für Online-Durchsuchung und Quellen-TKÜ für verfassungswidrig. Die höchsten Hürden für derartige Eingriffe, wie sie das BVerfG skizziert hat, wurden missachtet. Ein staatliches Ausnutzen von IT-Sicherheitslücken bleibt ein massiver Widerspruch zu sonstigen Bekenntnissen zur IT-Sicherheit. Backdoors stehen zum Glück gar nicht zur Debatte. Das würde die Vertrauenswürdigkeit der gesamten IT-Industrie schwer beschädigen.

CDU / CSU:
Die herkömmliche Telekommunikationsüberwachung führt oft nicht weiter, seitdem die Täter verschlüsselte Messenger-Dienste nutzen. Es macht keinen Sinn, wenn die Strafverfolger nur Ermittlungsmethoden einsetzen können, die am Täterverhalten völlig vorbeigehen. Deshalb haben sich CDU und CSU für neue Befugnisse eingesetzt, die den neuen Realitäten gerecht werden. Quellen-TKÜ und Onlinedurchsuchung sind gewichtige Grundrechtseingriffe, die aber gerechtfertigt sind, wenn es um schwere Kriminalität und Terrorismus geht. Die rechtlichen und auch die technischen Hürden

sind dabei so hoch, dass ihr Einsatz schon deshalb nur bei schwerer Kriminalität in Frage kommt. Die Anwendung der Quellen-TKÜ steht zudem unter Richtervorbehalt.

Aufgrund der eingeschränkten Anwendung wird die Gefahr für die allgemeine IT-Sicherheit daher als begrenzt angesehen. Schon gar nicht steht sie im Widerspruch zu dem herausragenden Anliegen, die IT-Sicherheit vor privaten Hackerangriffen zu erhöhen. „Made in Germany“ muss bei der Datensicherheit zum Gütesiegel werden. Unternehmen sollen sich für Deutschland entscheiden, weil hier Daten sicherer sind als anderswo.

Wir brauchen bundesweit eine Cybersicherheitsstrategie aus einem Guss. Wir bauen ein schlagkräftiges Cyberabwehrzentrum auf. Zusätzliche Internetpolizisten sollen Internet-und Computerkriminalität bekämpfen und das „Darknet“ stärker überwachen. Das dient besonders dem Schutz unserer Kinder und verhindert rechtsfreie Räume im Internet. Wirtschaft, Forschung und kritische Infrastrukturen müssen vor Internet-Attacken geschützt werden. Die Hersteller wollen wir verpflichten, ihre IT-Produkte dauerhaft sicher zu halten.

Die LINKE:
Einen Ausgleich zwischen dem Ziel eines höchstmöglichen Schutzes der IT-Infrastruktur und dem Ziel des verdeckten Zugriffs staatlicher Stellen auf IT-Systeme ist nicht möglich. Die staatliche Nutzung von Sicherheitsschwachstellen bedeutet nichts anderes, dass der Markt für Sicherheitslücken befördert wird und staatlichen Behörden neben Kriminellen als Gefährder der ITSicherheit auftreten. Aus diesem Grund fordern wir den Verzicht auf solche Eingriffsbefugnisse.

FDP:

Wir Freie Demokraten kämpfen gegen jede anlasslose Erhebung, Speicherung und Überwachung von personenbezogenen Daten – wie durch die anlasslose Vorratsdatenspeicherung. Eine lückenlose Überwachung unbescholtener Bürgerinnen und Bürger, gleich ob durch deutsche Sicherheitsbehörden oder fremde Nachrichtendienste, ist für uns nicht hinnehmbar. Deshalb wollen wir sowohl die Möglichkeiten zur Funkzellenabfrage als auch der Bestandsdatenauskunft deutlich einschränken. Beides soll grundsätzlich nur noch möglich sein, wenn ein Gericht es erlaubt. Denn auch die Bekämpfung von Terrorismus und Kriminalität rechtfertigt nicht die lückenlose Überwachung unbescholtener Bürgerinnen und Bürger.

Im Gegensatz zu mehr Überwachung als Datenbeschaffungsinstrument sind offensichtlich nicht die fehlenden Daten das Problem, wenn es um die Effektivität der Sicherheitsbehörden geht. Vielmehr mangelt es an Personal, um die Spuren zu verfolgen: Ein Großteil der Terroristen, die in den vergangenen Jahren in Europa Mordanschläge verübten, waren den Behörden bekannt – und dennoch konnten sie ihre Verbrechen begehen. Um das zu verhindern, müssen nicht noch mehr Daten unbescholtener Bürgerinnen und Bürger ohne konkreten Anlass gesammelt werden. Sinnvoller ist es, Gefährder gezielt zu identifizieren und lückenlos zu überwachen.

SPD:
Die SPD lehnt eine Einschränkung der freien Verfügbarkeit von Verschlüsselung oder die Verpflichtung der Unternehmen zum Einbau von Hintertüren oder Backdoors ab, denn vertrauenswürdige Verschlüsselungstechnologie ist eine grundlegende Voraussetzung für IT-Sicherheit und Backdoors würden die IT-Sicherheit grundsätzlich in Frage stellen.
Was die Frage des Trojaners anbelangt, so vertrete ich die Auffassung, dass dieser zur Abwehr von schwersten Straftaten zwar möglich sein muss, zugleich aber viel strikter begrenzt werden muss als in der jetzigen Regelung. Insgesamt bin ich der Auffassung, dass wir eine gesellschaftliche Diskussion brauchen, wie wir die Grundrechte in der digitalen Welt sicherstellen wollen. Dazu zählt angesichts der neuen technologischen Entwicklungen auch die Frage, ob die die Abwägung zwischen Freiheit und Sicherheit zum Teil nicht auch andere und neue Antworten und neue Grenzziehungen erfordert.

Frage 9:

Ende-zu-Ende-Verschlüsselung ist ein wichtiger Faktor der IT-Sicherheit. Inzwischen hat sogar Whats App dem Druck nachgegeben und Ende-zu-Ende-Verschlüsselung eingeführt. Andererseits wird mit der neuen Sicherheitsbehörde ZITIS zur Entschlüsselung der Online-Kommunikation genau diese Sicherheit wieder gefährdet. Wie wollen Sie die berechtigten Interessen von Bürgern und Unternehmen wahren?

Bündnis 90/Die Grünen:
Wir halten den Erhalt des offenen verschlüsselten Internet für verfassungsrechtlich wie demokratisch geboten. Vertrauliche Kommunikation ist die Grundlage moderner Demokratien. Staatliche Schwachstellenbeschaffung und/oder Ausnutzung in jeder Form wirft gravierende rechtliche Fragen auf, die ungeklärt sind. Vor diesem Hintergrund ist die Schaffung eines ZITIS in dieser Form unverantwortlich und abzulehnen. Denn es werden dort womöglich Verfahren und Tools produziert, für die es bei den anfragenden Behörden keine hinreichenden, verfassungsrechtlich tragfähigen Rechtsgrundlagen gibt.

Die LINKE:
Wie zu Frage 8 ausgeführt, lehnen wir den verdeckten staatlichen Zugriff auf IT-Systeme ab. Wir sprechen uns dafür aus, dass der Staat die Entwicklung frei zugänglicher Software zur Verschlüsselung von Kommunikation und Daten unterstützt und so einen Beitrag zur IT-Sicherheit für alle leistet.

CDU / CSU:
Leistungsfähige Verschlüsselungsprodukte sind heute unverzichtbar. Sie werden in der Wirtschaft, im Staat und von Bürgern eingesetzt, sei es bei Online-Finanztransaktionen oder sicheren Methoden zur Kommunikation. Eine staatlich verordnete Schwächung von Verschlüsselungsverfahren lehne ich ab.

FDP:
Wir Freie Demokraten fordern ein Grundrecht auf Verschlüsselung. Die Weiterentwicklung von Verschlüsselungstechnologien, der Sicherheit von Speichersystemen und von qualifizierten Zugriffs- und Berechtigungslogiken muss hierzu stärker vorangetrieben werden. Gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme lehnen wir genauso wie den Einsatz von Backdoors und die staatliche Beteiligung an digitalen Grau- und Schwarzmärkten ab.

SPD:

Die Verfügbarkeit von freier und vertrauenswürdiger Verschlüsselungstechnologie ist eine zentrale Voraussetzung für die Gewährleistung der IT-Sicherheit. Aus meiner Sicht ist die neue Sicherheitsbehörde ZITIS deswegen problematisch, weil es – anders als beispielsweise beim Bundesamt für Sicherheit in der Informationstechnik (BSI) keine gesetzliche Grundlage für ihre Tätigkeit gibt. Ich plädiere für eine Neuausrichtung des BSI als zentrale präventive und unabhängige Behörde zum Schutz der IT-Sicherheit, welche Bürgerinnen und Bürger, die Wirtschaft und die Verwaltung berät und unterstützt. Gleichzeitig plädiere ich dafür, eine klare gesetzliche Grundlage für die Sicherheitsbehörde ZITIS zu schaffen und den Auftrag sowie die notwendigen Begrenzungen festzuschreiben.