CDU/CSU
Thomas Jarzombek

1. Wie wichtig stufen Sie die Bedeutung der IT-Sicherheit ein:
a) für die Politik
b) für die Wirtschaft
c) für die Bürger

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.

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.

2a. Ja.
2b. Nein. Weder der Staat, noch die Bürger oder Unternehmen können IT-Sicherheit alleine sicherstellen.
2c. Nein. Weder der Staat, noch die Bürger oder Unternehmen können IT-Sicherheit alleine sicherstellen.
2d. *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.*

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?

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.

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 Landesdatenschutzbeauftragten sind personell unterbesetzt. Welche Maßnahmen wollen Sie einleiten um dies zu verbessern?

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.

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?

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.

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?

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

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?

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.

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?

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.

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?

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.