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

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

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.

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.

a) 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.

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?

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.

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?

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.

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?

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.

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?

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.

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?

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.

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?

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.

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?

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.