Fragenkatalog für das öffentliche Fachgespräch des Ausschusses Digitale Agenda des Deutschen Bundestages zum Thema „IT Sicherheit“ am Mittwoch, dem 7. Mai 2014

1. Der Ausspähskandal durch ausländische Nachrichtendienste, die zahlreichen Fälle von Identitätsklau und zuletzt die OpenSSL-Sicherheitslücke haben die Verletzlichkeit der digitalen Infrastrukturen offensichtlich gemacht. Inwieweit ist eine sichere Kommunikation über die bestehenden Infrastrukturen aus Ihrer Sicht heute überhaupt noch möglich? Welche Erkenntnisse gibt es zu den Angriffsmöglichkeiten und Kompromittierungen der Informations- und Kommunikationsinfrastruktur (Hard- und Software, Netzwerktechnik, Normen und Standards etc.)? Welche Maßnahmen (auch gesetzgeberische) müssen ergriffen werden, um den Grundrechtsschutz und die Vertraulichkeit der Kommunikation wieder sicherzustellen?

2. Welche Abwehrmöglichkeiten (Hard- und Software) stehen privaten Nutzerinnen und Nutzern, Unternehmen, Behörden und Verfassungsorganen heute zur Verfügung, um die eigene Datensicherheit in kompromittierten Kommunikationsinfrastrukturen zu erhöhen und welche Möglichkeiten gibt es für den Gesetzgeber, diese auszubauen?

3. Welche Maßnahmen können Anbieter/Betreiber von Kommunikationsdiensten und -infrastruktur ergreifen und welche Möglichkeiten gibt es für den Gesetzgeber, sie hierbei zu unterstützen?

4. Inwieweit kann die Sicherheit bei der Nutzung von Kommunikationsdiensten wie De-Mail, E-Mail und anderen Messaging-Diensten weiter erhöht werden? Wie werden die bisherigen gesetzlichen Grundlagen hierzu eingeschätzt? Welchen Beitrag können öffentliche Stellen (z. B. Bundesdruckerei, Bundesamt für die Sicherheit in der Informationstechnik) leisten, wenn diese Zertifikate zur Verschlüsselung zur Verfügung stellen würden?

5. Wie können Privatpersonen sowie klein- und mittelständische Unternehmen zur stärkeren Nutzung sicherer Kommunikationsverbindungen und Verschlüsselungsverfahren bewegt werden? Besteht hier politischer Handlungsbedarf?

6. Inwieweit besteht politischer Handlungsbedarf zur Verbesserung der Datensicherheit und des Datenschutzes bei neuen Kommunikationsdiensten wie mobilen Instant-Messengern (WhatsApp etc.)?

7. Welchen Beitrag können Vorschläge wie Deutschland-Mail oder Schengen-Routing tatsächlich leisten und müsste nicht die zentrale Maßnahme sein, schnell vertrauenswürdige und wirksame Ende-zu-Ende-Verschlüsselungen durchzusetzen? Welche Maßnahmen müssen ergriffen werden, um hierfür die jeweiligen Systemumgebungen abzusichern und zugleich die Handhabbarkeit zu erleichtern? Inwieweit sollten Telekommunikationsanbieter zu einer

Transportverschlüsselung verpflichtet werden?

8. Wo sehen Sie gesetzgeberischen Handlungsbedarf (z. B. im Strafrecht, aber auch im TKG, im TMG oder auch in den Sicherheitsgesetzen), um den Grundrechtsschutz und den Schutz der Vertraulichkeit der Kommunikation sicherzustellen?

9. Welchen Beitrag kann das Bundesamt für die Sicherheit in der Informationstechnik (BSI) zur Erhöhung der IT-Sicherheit und zur Unterstützung des Selbstschutzes der Bürgerinnen und Bürger sowie der Unternehmen leisten, welche Rahmenbedingungen müssen hierfür erweitert und welche personellen sowie materiellen Grundlagen geschaffen werden? Inwieweit müssen welche Kapazitäten des BSI und auch des Cyber-Abwehrzentrums ausgebaut werden? Wie kann das BSI in seiner Rolle als neutraler Berater der Bürgerinnen und Bürger gestärkt werden? Inwieweit ist eine effektive Koordinierung mit dem Bundesministerium des Innern und den anderen Ressorts der Bundesregierung gesichert?

10. Die gravierende Sicherheitslücke Heartbleed in OpenSSL ist auch ein Beleg dafür, welche Folgen es hat, wenn derart zentrale Funktionalitäten nicht unabhängig überprüft werden. Wie können beispielsweise angemessene IT-Sicherheitsaudits für Open-Source-Security-Software ermöglicht werden und wie können das BSI oder andere, auch nicht-staatliche Stellen, derartige Audits unterstützen?

11. Sehen Sie die Vorschläge der EU-Datenschutzgrundverordnung als ausreichend an, um ausländische Unternehmen (Facebook, Google, WhatsApp etc.), die in Europa ihre Dienste anbieten, zur Wahrung der europäischen Datenschutzgrundsätze zu verpflichten oder wo besteht hier aus Ihrer Sicht noch Handlungsbedarf? Welche Möglichkeiten bestehen, europäische Bürgerinnen und Bürger bei der Nutzung entsprechender Angebote vor dem Ausspähen durch ausländische Dienste zu schützen? Wie schätzen Sie weitere EU-Legislativen (z. B. die Cybercrime-Richtlinie) diesbezüglich ein?