Dr. Thomas Lapp

Von: Klingbeil Lars <lars.klingbeil@bundestag.de>
Gesendet: Freitag, 1. September 2017 13:47
An: Dr. Thomas Lapp
Betreff: Re: Fragen an die SPD zur Bundestagswahl und IT-Sicherheit

Sehr geehrter Herr Dr. Lapp,

gerne lasse ich Ihnen hiermit die Antworten von Herrn Klingbeil zukommen:

1. Wie wichtig stufen Sie die Bedeutung der IT-Sicherheit ein:
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.

2. Stimmen Sie folgenden Aussagen zu:
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 sich 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.

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?
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.

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

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 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.

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

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?
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.

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 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.

9. Ende-zu-Ende-Verschlüsselung ist ein wichtiger Faktor der IT-Sicherheit. Inzwischen hat sogar WhatsApp 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?
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.

Mit freundlichen Grüßen
Judith Gläser

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

Aktuelle Informationen und Termine – Newsletter abonnieren unter:
http://www.lars-klingbeil.de/aktuell/newsletter/
_____

Tel: (030) 227-71515
Fax: (030) 227-76452

Büro Lars Klingbeil, MdB
Platz der Republik 1
11011 Berlin

Von: "Dr. Thomas Lapp" <thomas.lapp@nifis.de>
Datum: Freitag, 25. August 2017 um 10:55
An: Klingbeil Lars <lars.klingbeil@bundestag.de>
Betreff: Fragen an die SPD zur Bundestagswahl und IT-Sicherheit

Sehr geehrter Herr Klingbeil,

als Mitglied des Bundestages und Obmann im Ausschuss digitale Agenda schreiben wir Sie an, um unseren Mitgliedern einen Eindruck von der Agenda Ihrer Partei und anderer Parteien zu geben. Sollte ein anderes Mitglied der Fraktion unsere Fragen eher beantworten können, nehmen wir gern zu diesem Kontakt auf. Sie können unseren Brief auch gern weiterleiten.

Für Ihre Unterstützung danken wir sehr. Wir werden die Antworten auf unsere Fragen in Gegenübestellung auf unserer Webseite und zusammengefasst in der Presse- und Öffentlichkeitsarbeit veröffentlichen.

Für Fragen stehe ich gern zur Verfügung.

--
Mit freundlichen Grüßen

Dr. Thomas Lapp - Rechtsanwalt und Mediator
Vorsitzender der NIFIS e.V.
Nationale Initiative für Informations- und Internetsicherheit

Berkersheimer Bahnstraße 5
60435 Frankfurt am Main
Tel.: +49 69 2444 4757
Fax: +49 69 2444 4746
Mobil: +49 700 RA DR Lapp (=+49 700 72 37 5277)
www.nifis.de
thomas.lapp@nifis.de
http://twitter.com/NIFIS