Dr. Thomas Lapp

Von: programm@fdp.de im Auftrag von Nicola Beer <programm@fdp.de>
Gesendet: Donnerstag, 14. September 2017 11:22
An: Thomas.Lapp@nifis.de
Betreff: Ihre Wahlprüfsteine zur Bundestagswahl 2017

Freie
Demol

Sehr geehrter Herr Dr. Lapp,

haben Sie vielen Dank für die Übermittlung Ihrer Wahlprüfsteine anlässlich der Bundestagswahl 2017, deren Eingang wir bereits bestätigt hatten.

Wir freuen uns sehr über Ihr Interesse an den Positionen der Freien Demokraten und nehmen zu Ihren Fragen beziehungsweise Forderungen gerne Stellung.

Im Folgenden übermittle ich Ihnen im Namen der Freien Demokraten unsere Antworten:

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

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.

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) Ja.
b) 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) 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) 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 empfohlenen Prozesse zum Einspielen von Updates befolgen.

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 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.

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 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.

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?

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.

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 beschräkt bleibt?

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.

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?

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.

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 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.

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 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.

Lassen Sie uns dazu auch nach der Bundestagswahl im Gespräch bleiben.

Mit freundlichen Grüßen

Ihre

Nicola Beer MdL
Staatsministerin a.D.
Generalsekretärin

Freie Demokratische Partei
Hans-Dietrich-Genscher-Haus
Reinhardtstraße 14, 10117 Berlin

T: 030 284958-269
programm@fdp.de
www.fdp.de