Wahlprüfstein DIE LINKE

NIFIS Nationale Initiative für Informations- und Internet-Sicherheit e.V.
Berkersheimer Bahnstr. 5
60435 Frankfurt am Main

DIE LINKE zu IT-Sicherheit

---

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

Hier kann es aus unserer Sicht keine Abstufung geben. IT-Sicherheit hat aus unterschiedlichen Gründen für die genannten Gruppen eine hohe Bedeutung, da wesentliche Teile den politischen, wirtschaftlichen und privaten Lebens ohne eine sichere und integre IT nicht mehr zu bewerkstelligen sind.

---

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. Dazu zählen für uns auch Vorschriften zur Härtung von IT-Systemen durch die Implementierung einer IT-Produkthaftung.
b) Ja
c) Mit Einschränkungen ja. Allerdings braucht es dafür einen klaren rechtlichen Rahmen, der die Verantwortlichkeit der Unternehmen und ihre Kooperation mit zuständigen staatlichen Stellen regelt.
d) Ja. IT-Sicherheit kann nur funktionieren, wenn alle sich nach ihren Möglichkeiten beteiligen, Bedrohungen einzudämmen.

---

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?

Die zahlreichen bestehenden Abkommen zur Rechtshilfe in Strafsachen müssen den neuen Gegebenheiten angepasst werden, insbesondere bei den bestehenden Regelungen auf Ebene der EU ist dabei auf eine strikt rechtsstaatliche Ausgestaltung zu achten. Allerdings werden wir damit leben müssen, dass sich Straftäter über die Nutzung von Infrastruktur in nicht kooperationswilligen oder –fähigen Staaten einer effizienten Strafverfolgung entziehen.

---

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?

Für die personelle Ausstattung der Datenschutzaufsicht in den Ländern sind diese selbst verantwortlich. Wir setzen uns dafür ein, dass sowohl im Bund als auch in den Ländern eine aufgabenadäquate personelle Stärkung vorgenommen wird. Bei Umsetzung unseres Steuerkonzepts erhalten die Länder die hierfür notwendigen finanziellen Spielräume.

---

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?

Für eine effektive Prävention gegen Bedrohungen der IT-Sicherheit müssen auch die Unternehmen ihren Verpflichtungen nachkommen, zu ihrer Durchsetzung braucht es auch die entsprechenden Behörden, also Bürokratie. Von vornherein zum

Scheitern verurteilte Mammutvorhaben wie DE-Mail haben wir immer abgelehnt.

---

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?

Wir haben alle Gesetze abgelehnt, die eine anlasslose Massenspeicherung von Daten eingeführt haben, wie die TK-Vorratsdatenspeicherung und die Fluggastdatenspeicherung. Nur höchstmögliche Datensparsamkeit bietet eine Gewähr gegen Missbrauch von Daten oder die später vorgenommen Ausweitung ihrer Nutzung.

---

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 sehen die Einführung bzw. verstärkte Implementierung des „elektronischen Identitätsnachweises“ kritisch. Angesichts von Bestrebungen in der gesamten EU, Möglichkeiten der eindeutigen elektronischen Authentifizierung zu finden, die sowohl von staatlicher Seite als auch etwa im Fernhandel zur Anwendung kommen können, wurde hier womöglich eine teure und am Ende wenig effiziente Insellösung geschaffen. Eine Alternative bestünde unseres Erachtens auf gerät- und plattformunabhängigen, offenen Lösungen. Wie diese aussehen können, muss tatsächlich in Kooperation aller Beteiligten entwickelt 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?

Einen Ausgleich zwischen dem Ziel eines höchstmöglichen Schutzes der IT-Infrastruktur und dem Ziel des verdeckten Zugriffs staatlicher Stellen auf IT-Systeme ist nicht möglich. Die staatliche Nutzung von Sicherheitsschwachstellen bedeutet nichts anderes, dass der Markt für Sicherheitslücken befördert wird und staatlichen Behörden neben Kriminellen als Gefährder der IT-Sicherheit auftreten. Aus diesem Grund fordern wir den Verzicht auf solche Eingriffsbefugnisse.

---

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?

Wie zu Frage 8 ausgeführt, lehnen wir den verdeckten staatlichen Zugriff auf IT-Systeme ab. Wir sprechen uns dafür aus, dass der Staat die Entwicklung frei zugänglicher Software zur Verschlüsselung von Kommunikation und Daten unterstützt und so einen Beitrag zur IT-Sicherheit für alle leistet.