Grüner Sechs-Punkte-Plan für IT-Sicherheit und Datenschutz

IT Sicherheit stärken – Freiheit sichern

Wir wollen, dass das Internet ein freier digitaler Ort bleibt, an dem sich die Menschen sicher bewegen können. IT-Sicherheit und Datenschutz im Netz sind unabdingbar für die Funktionsfähigkeit von Demokratie und Rechtsstaat im digitalen Zeitalter. Der Staat hat die Aufgabe, die verfassungsrechtlich verankerten Grundrechte zu achten und sich für den Schutz der Bürgerinnen und Bürger vor Gefahren einzusetzen. Das gilt für die analoge genauso wie für die digitale Welt. Erfolgreiche Angriffe auf IT-Systeme und digitale Infrastrukturen bis hin zum Netz der Bundesregierung, steigende Fallzahlen im Bereich Cybercrime und der jüngst bekannt gewordenen Hackerangriff mit der Veröffentlichung von persönlichen Daten von hunderten Politikerinnen und Politikern sowie Personen des öffentlichen Lebens zeigen: Wir brauchen höhere Schutzstandards, besseren Opferschutz und eine zielgerechte Prävention.

1. In einem **unabhängigen Beratungsnetzwerk** für Sicherheit in der Informationstechnik wollen wir alle bestehenden Informations- und Beratungsangebote von öffentlichen Stellen des Landes (z.B. Verbraucherzentrale, Landesbeauftragte für Datenschutz und Informationsfreiheit, Cybercrime-Kompetenzzentrum im LKA oder Forschungseinrichtungen) bündeln und durch neue Angebote ergänzen. Dazu gehören vor allem Informations- und Schulungsangebote für kleine und mittlere Unternehmen (KMU), Vereine und Verbände, eine „Task-Force Internet-Betrug“ als Frühwarnsystem sowie Hilfestellung für betroffene Opfer durch eine Hotline.
2. Durch **Förderprogramme** für Hochschulausgründungen wollen wir Unternehmensgründungen zur Stärkung der Internetsicherheit unterstützen. Hier gibt es viel Bedarf und es bieten sich für Gründerinnen und Gründer lohnende Geschäftsfelder, beispielsweise für anwenderfreundliche Verschlüsselungsmöglichkeiten für Kommunikation im Alltag und in der Wirtschaft.

3. Das Land muss **Schutzlücken schließen**, statt sie für das Auslesen von Kommunikation per Staatstrojaner durch die Polizei offen zu halten. Der Staat macht sich so selbst zum Hacker. Dabei nimmt er die Gefahr in Kauf, dass diese Lücken auch von Kriminellen für ihre Zwecke genutzt werden können. Da bisher keine technisch und verfassungsrechtlich sichere Spähsoftware existiert, darf der Staat diese Risiken für die IT-Sicherheit nicht eingehen.
4. Betreiber von großen Internetplattformen müssen verpflichtet werden, **Notfallkontakte bereitzuhalten**, um umgehend Profile sperren zu können, die für IT-Angriffe oder deren hauptsächliche Verbreitung gestohlener Inhalte verantwortlich sind. Ebenfalls müssen die Nutzerkonten von gehackten Geschädigten nach Bekanntwerden unverzüglich gesperrt werden können.
5. Für IT-Technik brauchen wir europäische Mindeststandards bei der Sicherheit. Hierfür fordern wir ein **IT-Sicherheits-Gütesiegel** der EU.
6. Geltende **Haftungsregelungen** bei Herstellung und Verkauf von Hard- und Software sowie bei Sicherheitsverletzungen von Dienstleistern müssen überprüft und gegebenenfalls verändert werden.