38. Ordentliche Bundesdelegiertenkonferenz
Hamburg, 21.-23. November 2014

Beschluss

Digitale Selbstbestimmung gewährleisten - Grenzenlose Überwachung stoppen!

Text„*Ein Mensch unter Beobachtung ist niemals frei; und eine Gesellschaft unter ständiger Beobachtung ist keine Demokratie mehr.*“
(SchriftstellerInnen Appell 2013)

Seit Juni 2013 werden wir mit immer neuen Enthüllungen zum größten Überwachungs- und Ausspähskandals der Geschichte konfrontiert; kaum fassbare und menschenrechtsverachtende, anlasslose und flächendeckende Überwachungsmaßnahmen werden öffentlich bekannt. Diese Praktiken der Überwachung werden von der amerikanischen NSA oder dem britischen GCHQ oft in Zusammenarbeit mit anderen westlichen Geheimdiensten, inklusive dem deutschen Bundesnachrichtendienst (BND), durchgeführt. Wir GRÜNE fordern ein Ende dieser Totalüberwachung. Daraus folgt eine strikte parlamentarische Kontrolle der Geheimdienste, eine lückenlose Aufklärung über die Zugriffe der Geheimdienste auf personenbezogene Daten im In- und Ausland, zwingend notwendige gesetzliche Klarstellungen bezüglich der Überwachungs-Befugnisse, einen sicheren Aufenthalt für Edward Snowden in Deutschland und Europa und einen besseren gesetzlichen Schutz von Hinweisgeberinnen und Hinweisgebern (Whistleblowern). Darüber hinaus muss die Bundesregierung den verfassungsrechtlich gebotenen Schutz der wichtigsten Kommunikationsinfrastruktur unserer Zeit gewährleisten, um unsere Grund-, Bürger- und Freiheitsrechte, insbesondere das Recht auf Privatsphäre und das Telekommunikationsgeheimnis, auch in der digitalen Welt durchzusetzen. Dies erfordert weitreichende politische und rechtliche Veränderungen, was den rechtlichen und technischen Schutz der Privatsphäre und die Datensicherheit angeht.

Wir GRÜNE fordern daher:

I. Rechtsstaat und Datensouveränität mit rechtlichen und diplomatischen Mitteln verteidigen

1. Straftaten gegen die Datensouveränität konsequent verfolgen

Straftaten gegen BundesbürgerInnen sind konsequent zu verfolgen - auch und gerade dann, wenn sie von ausländischen Geheimdiensten begangen werden. In den letzten Monaten bekannt gewordene Vorfälle und Programme müssen umfassend untersucht, der Sachverhalt vollständig ausermittelt und, wo möglich, den deutschen Gerichten zugeführt werden. Die entsprechend verantwortlichen Personen in Deutschland sind zu identifizieren und strafrechtlich zu verfolgen oder, falls sie diplomatischen Schutz genießen, entweder auszuweisen oder zur unerwünschten Person zu erklären. Gegen EU-Mitgliedsstaaten, deren Geheimdienste weiterhin Angriffe auf Informationssysteme anderer Mitgliedsstaaten unternehmen, muss ein Vertragsverletzungsverfahren angestrengt werden. Deutsche Ermittlungsbehörden sollten zur Aufdeckung der in Deutschland stattgefundenen Angriffe alle notwendigen Ressourcen einsetzen, insbesondere die Unterstützung des Cybercrime Center von Europol für entsprechende Ermittlungen anfordern, da dies nicht eigeninitiativ tätig werden darf.

2. Keine Duldung von und Kooperation mit rechtsverletzenden ausländischen Geheimdiensten
Jede Form der Duldung von und Kooperation deutscher Behörden mit ausländischen Geheimdiensten, die offensichtlich rechtswidrig BürgerInnen in Deutschland überwachen, muss umgehend eingestellt werden. Insbesondere dürfen die deutschen Geheimdienste nicht mit ausländischen Diensten Daten austauschen bzw. deren Datenerhebung im Inland unterstützen, wenn die ausländischen Dienste die Daten auf nicht nachweisbaren oder gesetzeswidrigem Weg erlangten und/oder sie einer Nutzung zuführen, die für deutsche Dienste verboten ist. Die Verhinderung der großflächigen Ausforschung von BürgerInnen in Deutschland muss von den deutschen Diensten als Teil der Spionageabwehr verstanden werden; entsprechende Methoden und Ressourcen sind einzusetzen. Die Kooperation mit anderen Geheimdiensten, z. B. über das EU-Intelligence Center (INTCENT), muss eingestellt werden, solange diese keine Rechtsgrundlage im EU-Recht hat und keine angemessenen rechtlichen Rahmenbedingungen und Praktiken der kooperierenden Geheimdienste vorliegen. Die Bundesregierung und die Europäische Kommission müssen sicherstellen, dass sich ausnahmslos alle EU-Mitgliedsstaaten und ihre Geheimdienste an geltende nationale und europäische (grund-)rechtliche Vorgaben halten. Wir brauchen unverzüglich europaweite und langfristig weltweite Mindeststandards für geheimdienstliche Eingriffe in Grundrechte und ein effektives Kontroll- und Sanktionsregime.

3. Informationelle Selbstbestimmung der BürgerInnen als Voraussetzung internationaler Zusammenarbeit
Unser Recht auf Privatheit und unsere Datensouveränität, das haben die Enthüllungen Edward Snowdens gezeigt, stehen derzeit massiv in Frage. Es ist gegen staatliche und nichtstaatliche Akteure, egal ob diese inner- oder außerhalb der EU beheimatet sind, mit allen zur Verfügung stehenden Mitteln zu verteidigen. Die Bundesregierung muss unmissverständlich deutlich machen, dass sie die Verletzung der Privatsphäre ihrer BürgerInnen nicht hinnimmt und hierauf entsprechend reagiert. Insbesondere sollte die Bundesregierung die vollumfängliche Beachtung der – auch verfassungsrechtlich gebotenen - Datensouveränität von BürgerInnen und Unternehmen zur Mindestbedingung von Zusammenarbeit machen, z. B. in Bezug auf die Bereitschaft zum Datenaustausch bei Sicherheitspartnerschaften, Freihandelsabkommen oder der Vergabe von öffentlichen Aufträgen. Der Abschluss eines Rahmenabkommens zum Datenschutz im Strafverfolgungsbereich zwischen der EU und den USA mit effektiven, durchsetzbaren Rechten für europäische BürgerInnen muss Bedingung für jede weitere Zusammenarbeit mit US-Behörden sein. Bestehende Datenaustauschabkommen, zum Beispiel bezüglich des Austauschs von Bank- oder Fluggastdaten, müssen vor dem Hintergrund der Erkenntnisse der letzten Monate aufgekündigt werden.

4. Deutsche Geheimdienste demokratisch einhegen und kontrollieren
Auch die Befugnisse der deutschen Geheimdienste und Sicherheitsbehörden sind, das hat eine entsprechende Anhörung namhafter Verfassungsrechtler des Parlamentarischen Untersuchungsausschuss des Deutschen Bundestages deutlich gemacht, gesetzlich einzuhegen und die praktische Umsetzung sehr viel effektiver zu kontrollieren, allen voran durch die Parlamente, in den Diensten selber, durch die Gesellschaft und die Judikative. Die Möglichkeiten der technischen Überwachung müssen klar eingegrenzt werden. Bekannt gewordene Praktiken, vor allem was den Einsatz gemeinsamer Programme mit ausländischen Diensten und offenbar gewordenen Ringtausch-System von rechtswidrig erlangten Daten angehen, sind mit verfassungsrechtlichen Vorgaben nicht zu vereinbaren und müssen daher umgehend eingestellt werden. Das bewusste Verbauen und Offenhalten von Sicherheitslücken und die Kompromittierung von Netzinfrastrukturen und Computern, sind zu untersagen..) Auch im Ausland dürfen grundsätzlich durch deutsche Dienste keine Praktiken eingesetzt werden, die im Inland verboten sind. Die parlamentarischen Kontrollgremien sind besser auszustatten und mit robusteren und konkreteren Befugnissen zu versehen. Die Information muss zukünftig umfassend und proaktiv, nicht bloß wie bis-

her unvollständig und nur auf direkte Nachfrage erfolgen. Die Transparenz und die Rechtsschutzmöglichkeiten von Betroffenen sind zu verbessern. Whistleblower verdienen effektiven rechtlichen Schutz, besonders, wenn sie Informationen offenlegen, die klar rechtswidriges Handeln bspw. von in- oder ausländischen staatlichen Behörden betreffen. Sowohl der NSU- als auch der NSA-Skandal haben ein mannigfaltiges Versagen der Dienste offenbart. Hieraus müssen wir Konsequenzen ziehen: Für das Bundesamt für Verfassungsschutz fordern wir eine vorübergehende Auflösung und eine anschließende Debatte, welche Kompetenzen in einer neu zu gründenden Stelle wie fortgeführt werden könnten. Den Militärischen Abschirmdienst (MAD) wollen wir abwickeln.

5. Unabhängigkeit der Institutionen
Die Bundesregierung wird endlich einen ersten wichtigen Schritt gehen, und die Bundesbeauftragte für Datenschutz und Informationsfreiheit aus der direkten Verantwortlichkeit des Bundesinnenministeriums herauslösen. Damit setzt sie die seit Jahren überfällige Unabhängigkeit, die von uns gemeinsam mit dem Europäischen Gerichtshof wiederholt eingefordert wurde, endlich um. Nun muss dringend eine den aktuellen Herausforderungen angemessene personelle und finanzielle Ausstattung beschlossen werden. Ein ähnlicher Schritt steht beim Bundesamt für Informationssicherheit (BSI) noch aus. Wir wollen auch dieses Bundesamt unabhängig vom Innenministerium stellen. Durch erweiterte Befugnisse und eine verbesserte personelle und finanzielle Ausstattung wollen wir sicherstellen, dass das Amt zukünftig den in den letzten Jahren massiv gestiegenen Herausforderungen gerecht werden und seine vielfältigen Aufgaben in angemessener Art und Weise wahrnehmen kann. Bisher weigert sich die Bundesregierung, diese Vorschläge umzusetzen.

II. Technische Datensicherheit in den Kern der politischen Gestaltung rücken

1. Staatliche Unterstützung für sichere Informationstechnik
Sowohl bei der Vergabe öffentlicher Aufträge als auch bei der staatlichen Forschungspolitik muss zukünftig ein Schwerpunkt auf die Entwicklung und Förderung sicherer – möglichst freier - Software gelegt werden. Bekannte Sicherheitsvorfälle bei Unternehmen sind als negative Bewertung bei der öffentlichen Beschaffung zwingend zu berücksichtigen. Das erfordert ein radikales Umdenken, denn statt durch Förderprogramme wie INDECT Unsicherheit und Überwachung finanziell zu unterstützen, muss der Fokus auf Landes-, Bundes- und Europaebene zukünftig auf der Förderung sicherer Technik liegen.
Dementsprechend ist es wichtig, einerseits die IT- und Datensicherheitsforschung im Rahmen staatlicher Institutionen zu fördern und in diese zu investieren, andererseits aber auch Anreize für unabhängige Sicherheitsforschung zu schaffen, ihre Erkenntnisse zur Verbesserung der Sicherheit aller einzusetzen. Diese Schwerpunktsetzung kann somit auch zur Veröffentlichung von Sicherheitslücken gegen den Wunsch des Herstellers führen.
Ein besonderer Schwerpunkt muss die Entwicklung und Verbreitung ebenso robuster wie benutzerfreundlicher Cryptosysteme bilden. Hier ist der Aufholbedarf groß. Der Staat soll in entsprechende Forschung und Ausbildung investieren, denn hierbei handelt es sich im wahrsten Sinne des Wortes um eine Schlüsseltechnologie im digitalen Raum. Wir brauchen endlich durchgehende Ende-zu-Ende-Verschlüsselung bei allen IT-Großprojekten. Nur so ist in den letzten Monaten massiv verloren gegangenes NutzerInnen-Vertrauen in die globale Internetinfrastruktur langfristig zurückzugewinnen und Datensouveränität effektiv zu gewährleisten. Gerade in diesem Bereich sollte darüber nachgedacht werden, gezielte Förderprogramme für freie und offene Software zu entwickeln, um die Nachprüfbarkeit des Quellcodes, die Weiterentwicklung und -nutzbarkeit von Produkten zu sichern.

Langfristige Forschungsschwerpunkte sollten auch auf "Software-Verifikation" liegen und eine Offensive für hier vor Ort entwickelte und produzierte Technologie angestrebt werden (z. B. in

der Chip-, Netzwerk- und Speichertechnik). Deutschland sollte hier - auch vor dem Hintergrund des hohen deutschen Datenschutzniveaus - innerhalb Europas eine Vorreiterrolle einnehmen. Zwingend einhergehen muss dies mit dem klaren gesetzlichen Verbot an Geheimdienste und andere Sicherheitsbehörden, Einfluss auf die Forschung und Entwicklung solcher Technik zu nehmen. Deutsche und europäische Ausschreibungsbestimmungen müssen überprüfbar sichere IT beinhalten, etwa durch Bevorzugung von Open-Source-Lösungen.

2. Einführung einer gesetzlichen Pflicht, Sicherheitslücken umgehend zu beheben
Es bedarf einer umfassenden Meldepflicht für Sicherheitsvorfälle im IT-Bereich. Zudem bedarf es einer Verbesserung der Überprüfbarkeit von Software durch den Zwang, anders als bisher mit Sicherheitsproblemen umzugehen. Es muss eine gesetzliche Verpflichtung geben, Schwachstellen umgehend zu melden und schnellstmöglich zu beheben. Im Bereich offener Software sollte der Staat Systeme zur schnellen Behebung fördern und eine öffentlich einsehbare Warnliste mit entsprechend bekannten Problemen pflegen. Außerdem treten wir für Änderungen der Haftungs- und Gewährleistungsregeln ein, um Unsicherheit signifikant teurer zu machen als Untätigkeit. Die Haftung sollte für Herstellung und Vertrieb von Software gelten, die nicht auf quelloffener Software basiert. Dabei sollten nicht die Schwachstellen selbst zu einer Sanktion führen, sondern nur der falsche Umgang mit Sicherheitsproblemen. Voraussetzung der Haftung für Sicherheitslücken sollte sein, dass diese trotz Kenntnis des Verantwortlichen nicht in angemessener Zeit gemeldet und geschlossen worden sind.
Die Meldepflichten im geplanten IT-Sicherheitsgesetz und in der sich kurz vor dem Abschluss befindlichen Netzwerk- und Informationssicherheits-Richtlinie der EU sind ein Schritt in die richtige Richtung, greifen aber zu kurz, weil sie nur neue Sicherheitsvorfälle adressieren, darüber hinaus aber keine Regeln zum Umgang mit bekannten Schwachstellen enthalten. Zudem sollen sie nur für Unternehmen, nicht jedoch für staatliche Stellen gelten. Die Bundesregierung muss sich bei ihrem eigenen Gesetz und im Ministerrat für die europäische Richtlinie dafür einsetzen, dass auch bekannt gewordene Schwachstellen angegangen und auch staatliche Stellen zur Meldung und Schließung von Lücken verpflichtet werden.
Eine besondere Verpflichtung haben die Zertifizierungsstellen (Certificate Authorities, CA). Sie sind für das Erstellen, die Ausgabe, Verwaltung und Sperrung von digitalen Zertifikaten zuständig. Werden von ihnen technische Schwachstellen bewusst verschwiegen und nicht umgehend behoben und nach deren Beseitigung öffentlich gemacht, so muss neben empfindlichen Geldstrafen auch die Möglichkeit weiterer, effektiver Sanktionen wie dem Strafrecht bestehen.

3. Gesetzliche Gewährleistung des Rechts, Unsicherheit thematisieren zu dürfen
Wir wollen das Aufdecken technischer Schwachstellen fördern. Wer Sicherheitslücken aufdeckt, den Hersteller informiert und ihm eine angemessene Zeit zur Korrektur einräumt, bis er die Sicherheitslücke veröffentlicht (sog. Responsible Disclosure), darf hierfür nicht bestraft oder kriminalisiert werden. Es muss vielmehr Unterstützung und Anreize geben, technische Unsicherheit aufzudecken und klar zu benennen, um mögliche Schäden so klein wie möglich zu halten. Um dieses Ziel zu erreichen, darf es kein generelles Verbot von Hackertools geben. Wir wollen außerdem keine Kriminalisierung des umfassenden Aufdeckens von Sicherheitslücken (Full-Disclosure-Ansatz). Entscheidend ist die Differenzierung bei der Ausnutzung dieses Wissens, das heißt zu unterscheiden, ob es z. B. zur Schädigung Dritter genutzt wird oder es legitimer Sicherheitsforschung dient.

4. Mitwirkung staatlicher Stellen bei der Gewährleistung von IT-Sicherheit
Es muss staatlichen Stellen untersagt sein, die Sicherheit und Integrität von IT-Produkten und der Kommunikationsinfrastruktur negativ zu beeinflussen. Keinesfalls dürfen staatliche Institutionen und insbesondere Geheimdienste den Schwarzmarkt für Sicherheitslücken befördern, indem sie dort als Käufer oder Verkäufer auftreten. Vielmehr muss gelten: Sobald eine staatliche Institution Kenntnis von einer Sicherheitslücke erlangt, muss sie verpflichtet sein, diese schnellst-

möglich zu melden und zu ihrer Beseitigung beizutragen. Das heißt, den Hersteller in Kenntnis zu setzen, auf die Beseitigung der Sicherheitslücke zu drängen, ggf. auch die Öffentlichkeit zu warnen und bei offener Software mit ihren Möglichkeiten zu unterstützen, die Schwachstellen zu beheben.

5. Einzelne NutzerInnen stärken

Wir sagen klar: Die bekannt gewordenen Praktiken verschiedener westlicher Geheimdienste, die eng mit großen IT-Firmen kooperieren und unsere Rechner und Kommunikationsinfrastruktur weitreichend kompromittiert haben, müssen vor allem tiefgreifende gesetzgeberische Konsequenzen mit dem Ziel der Wiederherstellung der Herrschaft des Rechts nach sich ziehen. Gleichzeitig kann ein effektiver Schutz der eigenen Daten und IT Struktur ein Baustein sein, die eigene Datensouveranität zu stärken. Neben der staatlichen Unterstützung für eine sichere technische Software- und Hardwareinfrastruktur muss es auch Wege zur Stärkung der einzelnen NutzerInnen geben. Dazu gehören beispielsweise ein effektives modernisiertes Datenschutzrecht, der Schutz und der Ausbau der informationellen Selbstbestimmung, eine den Herausforderungen angemessen ausgestattete Datenschutzaufsicht sowie der Ausbau entsprechender Bildungsangebote auf allen Ebenen wie auch weitreichende Auskunftsrechte für die Betroffenen. Eine Nutzung von Internetdiensten und Telemedienangeboten unter Pseudonymen oder anonym muss weiterhin möglich sein. Wir wollen die informationelle Selbstbestimmung auch dadurch stärken, dass Datenhehlerei als Straftatbestand eingeführt wird. Um europaweit einen starken Datenschutz mit echten Durchsetzungsmöglichkeiten zu bekommen, muss das Bundesinnenministerium sich endlich konstruktiv und ergebnisorientiert an den Verhandlungen zur EU-Datenschutz-Grundverordnung beteiligen.

Debatte vorantreiben

Die Digitalisierung aller Lebensbereiche geht einher mit einer zunehmenden Automatisierung. Diese Entwicklungen schreiten voran und haben weitreichende Auswirkungen auf unsere informationelle Selbstbestimmung aber auch auf unsere Arbeitswelt, unser soziales Zusammenleben, unsere Wirtschaft und unser Alltagsleben. Wir Grüne stehen dabei an vielen Stellen vor zahlreichen neuen Herausforderungen und vor Fragen auf die wir noch keine abschließenden Antworten haben. Um den Diskussionsprozess über diese Entwicklungen voranzutreiben und Antworten zu erarbeiten, werden die BAGen und der Bundesvorstand gebeten, diesen Diskussionsprozess mit einer eigenen Veranstaltung zu begleiten.