Piratenpartei Deutschland • Pflugstraße 9a • 10115 Berlin

Bundesgeschäftsstelle
Pflugstraße 9a
10115 Berlin

Ansprechpartner:

Dr. Patrick Breyer

Bundesministerin der Justiz und für
Verbraucherschutz
Frau Dr. Katarina Barley
Mohrenstraße 37
10117 Berlin

Kiel, 16.01.2019

Cyber-Sicherheitspaket zum Schutz vor Ausspähen privater Daten

Sehr geehrte Frau Bundesministerin,

die jüngste Veröffentlichung privater Daten von Politikern, Journalisten und Prominenten hat das öffentliche Vertrauen in die Sicherheit und Zuverlässigkeit unserer digitalen Infrastruktur erschüttert. Private Informationen in unbefugten Händen können hohe Funktionsträger erpressbar machen und ihr persönliches Umfeld sowie ihre Kontakte in Gefahr bringen.

Das Internet verbindet heute nicht nur die weltweite Wirtschaft. Es ist auch die Infrastruktur, auf die wir etwa zur Kommunikation und für den Zugang zu Informationen täglich angewiesen sind. Die Sicherheit und Zuverlässigkeit unserer gemeinschaftlichen Infrastruktur muss deswegen im Mittelpunkt politischen Anstrengungen stehen.

Die bisherigen politisch vorgeschlagenen Konsequenzen aus dem Doxxing-Fall (z.B. Einführung eines Siegels oder Ausweitung von Behördenkompetenzen) erscheinen nicht ausreichend oder ungeeignet, um weitere Fälle des Ausspähens von Daten zu verhindern.

Aus diesem Grund haben wir in einem digitalen Beteiligungsprozess ein Cyber-Sicherheitspaket zum Schutz vor Ausspähen privater Daten erarbeitet.

Das 17 Maßnahmenfelder umfassende Papier übersende ich Ihnen in der Anlage verbunden mit der Bitte, in einen Dialog mit der Zivilgesellschaft über unsere Sicherheit im Zeitalter der Digitalen Revolution einzutreten.

Mit freundlichem Gruß

Dr. Patrick Breyer

Anlage:

CYBER-SICHERHEITSPAKET ZUM SCHUTZ VOR AUSSPÄHEN PRIVATER DATEN

1. RECHT AUF DIGITALE MÜNDIGKEIT

Zur digitalen Mündigkeit und Selbstbestimmung gehört die Kompetenz, sich vor Ausspähung und Datenmissbrauch schützen zu können (digitale Selbstverteidigung). Die Vermittlung dieser Kompetenz in Bildungseinrichtungen und auf andere Weise (z.B. Cryptoparties) ist zu fördern und zu unterstützen.

2. RECHT AUF ANONYMITÄT

Informationstechnologie muss anonym nutzbar sein und bleiben. Whistleblower, Stalking-Opfer und andere sind auf Anonymität angewiesen. Im Gegensatz zu Klarnamenspflichten oder der zwingenden Erhebung von Identifizierungsmerkmalen (z.B. Rufnummer) schützt nur Anonymität wirksam vor Diebstahl, Verlust und Missbrauch persönlicher Daten. Auf europäischer Ebene ist ein Recht auf anonyme Nutzung von Telemedien und ein Verbot der Vorratsspeicherung des Nutzungsverhaltens einzuführen.

3. RECHT AUF BESEITIGUNG VON SCHWACHSTELLEN

Der Einbau von Schwachstellen (Hintertüren) ist zu verbieten.

Kommerzielle Hersteller von Informationstechnologie sowie kommerzielle und staatliche Anbieter von Telekommunikations- und Telemediendiensten werden verpflichtet, Schwachstellen nach Bekanntwerden zu beseitigen - für angemessene Zeit auch nach Einstellung des Vertriebs eines Produkts. Bei Verletzung dieser Pflicht werden sie für Schäden haftbar gemacht.

Entscheidet ein kommerzieller Hersteller, ein weit verbreitetes Produkt nicht weiterzuentwickeln, so hat er den Quelltext des Codes und möglichst auch die Entwicklungswerkzeuge zu veröffentlichen, damit die Öffentlichkeit Schwachstellen selbst beseitigen kann.

4. MELDEPFLICHT FÜR SCHWACHSTELLEN

Öffentliche Behörden werden verpflichtet, Schwachstellen offenzulegen, die ihnen bekannt werden.

5. RECHT AUF SICHERE VOREINSTELLUNG

Gebrauchsfertige Geräte zur Internetnutzung sowie kommerzielle Internetdienste müssen von ihrem Hersteller bzw. Anbieter so voreingestellt und bereit gestellt werden, dass die Vertraulichkeit, Verfügbarkeit und Unversehrtheit der Nutzerdaten dauerhaft nach den anerkannten Regeln der Technik gewährleistet ist (z.B. automatische Sicherheitspatches, Firewall, Schadprogrammerkennung). Der Nutzer muss dabei stets die volle Kontrolle über Vorkehrungen zu seinem Schutz behalten und diese auch abschalten können.

6. PRIVACY BY DESIGN FÜR IT-HERSTELLER

Kommerzielle informationstechnische Produkte zur Verarbeitung personenbezogener Daten müssen hierzulande so voreingestellt vertrieben werden, dass der Verwender das Datenschutzrecht einhält. Die DSGVO verpflichtet bisher nur die Datenverarbeiter zu einer datenschutzfreundlichen Technikgestaltung, nicht aber die Hersteller.

7. SCHUTZ VOR KOPPELUNG UND EINWILLIGUNGSKLAUSELN

Die Inanspruchnahme von Diensten darf nicht an die Einwilligung zur Preisgabe, Nutzung oder Weitergabe von Daten zu anderen Zwecken (z.B. Werbung) gekoppelt werden.

Verbraucher sind vor unangemessenen Datenverarbeitungs-Einwilligungsklauseln zu schützen, indem klargestellt wird, dass derartige Klauseln einer gerichtlichen Kontrolle unterliegen.

8. RECHT AUF SICHERHEITSTOOLS

Das Verbot von Werkzeugen für Sicherheitstests („Hackertools“) ist aufzuheben. Diese Tests sind zur Aufdeckung und Beseitigung von Schwachstellen unverzichtbar.

9. RECHT AUF VERSCHLÜSSELTE KOMMUNIKATION

Kommerzielle Hersteller von Telekommunikations-Endgeräten und von Software zur Telekommunikation (z.B. Messenger) werden verpflichtet, eine sichere Ende-zu-Ende-Verschlüsselung vorzunehmen, wenn sie auch vom Gesprächspartner unterstützt wird. Dies verhindert unbefugtes Abfangen beim Anbieter.

Betreiber von Übertragungsleitungen, insbesondere von internationalen Übertragungswegen, werden verpflichtet, eine sichere Transportverschlüsselung vorzunehmen. Dies verhindert unbefugtes Abfangen auf dem Übertragungsweg, insbesondere durch ausländische Geheimdienste. Die entsprechenden Vorschläge des Europäischen Parlaments zur ePrivacy-Reform (Art. 17) sind zu unterstützen.

Behörden und kommerzielle Anbieter von Telemedien werden verpflichtet, auch außerhalb von Systemen wie DE-Mail E-Mail-Kommunikation unter Verwendung anerkannter Verschlüsselungsstandards wie PGP zu ermöglichen.

10. RECHT AUF VERSCHLÜSSELTE DATENSPEICHERUNG

Kommerzielle Hersteller von Informationstechnologie sowie kommerzielle und staatliche Anbieter von Telekommunikations- und Telemediendiensten werden verpflichtet, Zugangsdaten und Nutzerdaten (einschließlich Metadaten) nach dem Stand der Technik zu schützen, insbesondere verschlüsselt zu speichern.

11. RECHT AUF TRANSPARENZ

Käufer von Informationstechnologie sowie Nutzer kommerzieller und staatlicher Telekommunikations- und Telemediendienste erhalten einen Anspruch auf Auskunft über die technisch-organisatorischen Maßnahmen zum Schutz ihrer Daten. So können die Nutzer aktiv Sicherheitsvorkehrungen einfordern oder zu einem sichereren Angebot wechseln.

12. RECHT AUF WEGWERFNUMMERN

Telefonnummern zur zeitlich begrenzten Weiterleitung an private Rufnummern sind identifizierungsfrei zuzulassen. Mithilfe von Wegwerfnummern können Privatnummern geschützt werden.

13. RECHT AUF „BEIPACKZETTEL“

Gebrauchsfertigen Geräten zur Internetnutzung sollten einfache Hinweise zur Vorbeugung häufiger Internetdelikte und zur richtigen Reaktion darauf beigefügt werden.

14. SICHERHEIT VON PASSWÖRTERN

Kommerzielle Hersteller von Informationstechnologie sowie kommerzielle und staatliche Anbieter von Telekommunikations- und Telemediendiensten werden verpflichtet, Mindestanforderungen an die Sicherheit von Passwörtern durchzusetzen, ohne die anonyme Nutzbarkeit zu beeinträchtigen.

Ist zu befürchten, dass Unbefugte Zugriff auf Zugangsdaten hatten, ist für die Vergabe neuer Zugangsdaten Sorge zu tragen.

15. RECHT AUF ANBIETERWECHSEL

Verbreitete kommerzielle soziale Netzwerke und Messengerdienste sind zur Zusammenschaltung zu verpflichten, so dass auch nach einem Anbieterwechsel die Kommunikation mit den Kontakten eines Nutzers möglich bleibt (Interoperabilitätspflicht). Nur so kann die Abhängigkeit von monopolartigen Anbietern wie Facebook überwunden werden.

16. DURCHSETZUNG DER DATENSPARSAMKEIT

Wettbewerber, Verbraucherzentralen und Datenschutzverbände erhalten das Recht, Datenschutzverstöße kommerzieller Anbieter von Internetdiensten abzumahnen.

17. RECHT AUF ENTSCHÄDIGUNG

Bei Verlust persönlicher Daten durch kommerzielle Anbieter von Internetdiensten erhalten Betroffene einen Anspruch auf pauschale Mindestentschädigung (z.B. 200 Euro pro Person). Dies setzt einen finanziellen Anreiz zur Gewährleistung der Datensicherheit und macht eine kollektive Rechtsdurchsetzung durch Musterfeststellungsklagen möglich.