Antrag 103/II/2023 Forum Netzpolitik
Ein starkes Recht auf Verschlüsselung zum Schutz der Bürger:innen und sensibler Unternehmensdaten

Beschluss: Annahme

Die Mitglieder der SPD-Fraktion im Bundestag und des Europaparlaments werden aufgefordert, folgenden Beschluss umzusetzen:

Wir bekennen uns klar zum Recht auf sichere Kommunikation und wirksame Verschlüsselung für alle Bürger:innen, Unternehmen und Institutionen: Als Bürger:innen haben wir das Recht, unsere persönlichen Informationen, Kommunikation und Daten durch Nutzung von Verschlüsselungstechnologien vor unbefugtem Zugriff zu schützen. Wir verlangen, dass das im Koalitionsvertrag auf Bundesebene vereinbarte Recht auf Verschlüsselung ohne Einschränkungen auf Bundes- und EU-Ebene umgesetzt wird.

Starke Verschlüsselungstechnologien werden aufgrund der zunehmenden Digitalisierung aller Lebensbereiche immer wichtiger. Sie schützen unsere private Kommunikation und persönliche Daten, schützen vor Massenüberwachung und Cyberkriminalität. Wir verlangen daher, dass die Politik Maßnahmen ergreift, um sicherzustellen, dass die Lebensbereiche online genauso geschützt sind wie offline.

Zum Recht auf sichere Kommunikation und wirksame Verschlüsselung gehört auch der Schutz der Kommunikation vor staatlicher Kontrolle. Eine Aufweichung oder Aushebelung der Ende-zu-Ende-Verschlüsselung durch freiwilliges oder verpflichtendes Client-Side-Scanning bei Anbietern verschlüsselter Kommunikationsplattformen ist daher nicht akzeptabel.

Im Einzelnen werden wir uns für die folgenden Punkte einsetzen:

1. Das grundlegende Schutzniveau muss gestärkt statt abgeschwächt werden: Es ist der staatliche Auftrag, die Schutzmechanismen aller zu erhöhen, statt sie zu begrenzen oder abzuschwächen. Regulierungen, die den Einbau von staatlichen Hintertüren als „goldene Schlüssel“ in Verschlüsselungstechnik oder andere generelle Abschwächungen des Schutzniveaus mit sich bringen würden, etwa zur Bekämpfung von Kriminalität, lehnen wir ab. Aktivitäten auf Bundes- oder EU-Ebene, die Verschlüsselung schwächen und umgehen, sind unzulässig, da sie die Sicherheit aller Bürger:innen und unserer Wirtschaft einem enormen Risiko aussetzen. Entsprechend werden auch aktuelle Bestrebungen auf EU-Ebene abgelehnt, die im Rahmen einer hochrangigen Expertengruppe (HLEG) im Juni 2023 durch die Ratspräsidentschaft eingerichtet wurde und technische Vorschläge für eine Regulierung zu Kryptoprodukten und -diensten zu entwickeln.
2. Wir wollen die technische Verfügbarkeit von Verschlüsselungstechnologie sicherstellen und erhöhen: Auf EU- und Bundesebene sollen künftig gezielt Open-Source-Projekte gefördert werden, die sich auf sichere Kommunikation und Verschlüsselungstechnologien konzentrieren oder sie beinhalten. Das erfolgt insbesondere durch finanzielle Mittel, Wettbewerbe, Auszeichnungen und Belohnungssysteme für die Suche nach Softwarefehlern (Bug Bounty). In dem Zusammenhang sollen auch Partnerschaften mit Unternehmen und Organisationen der Zivilgesellschaft gefördert werden. Forschungsprojekte im Bereich der Verschlüsselung sollen stärker gefördert werden. Wir unterstützen die Entwicklung und Nutzung von sicheren Kommunikations-Plattformen, die Ende-zu-Ende-Verschlüsselung bieten. Im Rahmen einer offenen Beschaffungspolitik müssen Lösungen für sichere und verschlüsselte Kommunikation, die auf offenen Standards und Open Source basieren, bei der Beschaffung von Software und Technologie für staatliche Einrichtungen bevorzugt werden. Zusätzlich müssen Maßnahmen ergriffen werden, damit entsprechende Software-Projekte durch Förderung, Sandbox-Nutzungen in Behörden etc. entsprechende Marktreife erreichen können.
3. Kampagnen zur Sensibilisierung und Aufklärung über die Vorteile von sicherer Kommunikation und Verschlüsselung und die Bedeutung der digitalen Sicherheit für Bürger:innen, mittelständische Unternehmen, Freiberufler:innen und Organisationen der Zivilgesellschaft, mit dem Ziel der stärkeren Nutzung entsprechender Technologien. Verschlüsselung muss die Regel werden, darf nicht die Ausnahme bleiben.

4. Starke Verschlüsselung als außenpolitisches Mittel zum weltweiten Schutz vor Zensur und Unterdrückung: Starke Verschlüsselung ermöglicht es Menschen, vertraulich und sicher miteinander zu kommunizieren, ohne Angst vor Überwachung oder Repressalien zu haben. Dies ist besonders wichtig in Ländern mit restriktiven Regimen, in denen die Meinungsfreiheit eingeschränkt ist. Menschen in zensierten Ländern helfen diese Techniken, auf Informationen und Nachrichten zuzugreifen, die sonst durch Zensurbehörden blockiert würden. Entsprechend sind diplomatische Kanäle zu nutzen, internationale Foren genutzt werden, Aktivist:innen und Zivilgesellschaft in entsprechenden Ländern Unterstützung angeboten werden.

5. Kommunikation und persönliche Daten müssen bereits heute durch zukunftstaugliche quantenresistente kryptografische Verfahren abgesichert werden: Angriffe auf heutige Verschlüsselungstechnik werden im Laufe der Zeit immer besser. Damit heute verschlüsselte Daten auch bei der Verfügbarkeit von Quantencomputern geschützt bleiben, muss Kommunikation bereits heute durch quantenresistente kryptografische Verfahren abgesichert werden. Insbesondere Bürger:innen, mittelständische Unternehmen, Freiberufler:innen und Organisationen der Zivilgesellschaft sind über quantenresistente Kommunikation und Speicherung aufzuklären und deren Einsatz ist zu fördern.

Überweisen an

Bundesparteitag 2023

Stellungnahme(n)

Beschluss des BPT 2023:

Überweisung an SPD-Bundestagsfraktion/SPD-Fraktion im EP