Deutscher Bundestag **Drucksache 20/12005**

20. Wahlperiode 26.06.2024

Antrag

der Abgeordneten Anke Domscheit-Berg, Dr. André Hahn, Gökay Akbulut, Clara Bünger, Nicole Gohlke, Susanne Hennig-Wellsow, Ina Latendorf, Cornelia Möhring, Petra Pau, Sören Pellmann, Martina Renner, Dr. Petra Sitte, Kathrin Vogler und der Gruppe Die Linke

IT-Sicherheitsforschung entkriminalisieren – Computerstrafrecht reformieren

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Durch die zunehmende Vernetzung von Staat, Wirtschaft und Gesellschaft sowie die steigende Nutzung digitaler Anwendungen und Dienstleistungen, vergrößern sich auch Risiken für die IT-Sicherheit. So beschreibt das BSI zur Lage der IT-Sicherheit in Deutschland 2023 die Bedrohungslage im Cyberraum so hoch wie nie zuvor, etwa 27.000 neue Schwachstellen in Softwareprodukten wurden bekannt, ein Zuwachs von 24 Prozent innerhalb eines Jahres (s. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html). Ursachen sind u.a. die zunehmende Komplexität von IT-Systemen, Fehler in der Programmierung, schwache Default-Einstellungen von IT-Produkten und fehlkonfigurierte Sicherheitseinstellungen. Schwachstellen in der IT-Infrastruktur sind ein großes Sicherheitsrisiko, denn sie können für Angriffe auf Computersysteme und deren Infiltrierung ausgenutzt werden. Gelangen Hersteller in Kenntnis derartiger Schwachstellen, können sie diese im Regelfall durch Sicherheitsupdates schließen, und damit deren künftige Ausnutzung für kriminelle Zwecke verhindern. Da Hersteller nicht alle Sicherheitslücken selbst finden, sind sie dafür auf verantwortliche Meldungen von Schwachstellen angewiesen.

Für das Aufspüren von Sicherheitslücken sind Hinweise Dritter aus der Zivilgesellschaft, Wirtschaft, Wissenschaft und/oder von Einzelpersonen wie durch ehrenamtliche IT-Sicherheitsforschende elementar (s. exemplarisch https://taz.de/IT-Experte-wird-angezeigt/!5808171/ und https://cispa.de/aepic). Obwohl das BSI als Meldestelle für Sicherheitsmängel mittlerweile auch anonyme Hinweise entgegennehmen darf, sind Personen, die aus guten Motiven solche Mängel und Lücken gezielt suchen, weiterhin der Gefahr der Strafverfolgung ausgesetzt. Die Suche nach Sicherheitslücken in IT-Systemen lässt sich jedoch nicht ausschließlich in praxisfernen „Laborumgebungen“ und auf Grundlage theoretischer Überlegungen durchführen.

Bisher ist für die Strafbarkeit allein der Umstand entscheidend, dass z. B. Software potenziell dazu genutzt werden könnte, in fremde Computer einzudringen, da keinerlei Ausnahmetatbestände bestehen, die einen solchen Einsatz straffrei

gestatten. Forschende sehen erhebliche Risiken darin, dass Ermittlungsbehörden aufgrund oberflächlicher Eindrücke einen Anfangsverdacht bejahen, auf dessen Grundlage dann erhebliche Eingriffe in die Grundrechte der IT-Sicherheitsforschenden erfolgen könnten (s. Whitepaper zur Rechtslage der IT-Sicherheitsforschung unter https://sec4research.de/assets/Whitepaper.pdf). Wenn IT-Sicherheitsforschende deshalb weniger IT-Sicherheitslücken suchen und finden, sinkt das IT-Sicherheitsniveau in Deutschland und gesamtgesellschaftlich steigen die Risiken bei anhaltender Zunahme der Bedrohungslage, die auch im Anstieg hybrider Angriffe durch drittstaatliche Stellen besteht.
Die Kriminalisierung legitimer IT-Sicherheitsforschung und der aktuelle Umgang mit IT-Sicherheitslücken führt zu einer Absenkung des IT-Sicherheitsniveaus in Deutschland. Trotz der Ankündigung im Koalitionsvertrag, dass die IT-Sicherheitsforschung legal durchführbar werden soll und trotz mehrerer interner Sondierungen sowie Expert:innen-Workshops, hat die Bundesregierung bis heute keinen Entwurf zur Novellierung des Computerstrafrechts vorgelegt.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

zeitnah einen Gesetzentwurf vorzulegen, der die Untersuchung, Aufdeckung sowie die Meldung von IT-Sicherheitslücken durch natürliche oder juristische Personen straffrei ermöglicht (z. B. durch die Einführung von Tatbestandsausschlüssen), sofern die Handlungen dem Ziel der ethisch verantwortungsvollen Erforschung, Identifizierung, Meldung und Schließung von IT-Sicherheitslücken in Hard- und Software dienen und die Handlungen keiner schädlichen oder böswilligen Intention unterliegen.

Berlin, den 25. Juni 2024

Heidi Reichinnek, Sören Pellmann und Gruppe

Begründung

Die aktuelle Ausgestaltung des Computerstrafrechts verursacht praktische Sorgen der IT-Sicherheitsforschung bei der Identifizierung, Meldung und Behebung von Sicherheitslücken. Eine Novellierung ist dringend erforderlich, um IT-Sicherheitsforschende in Deutschland zu entkriminalisieren und damit die Grundlagen für eine sichere digitale Infrastruktur zu schaffen. Wie der Wissenschaftliche Dienst des Deutschen Bundestag in seinem jüngsten Gutachten (s. WD 7 – 3000 – 104/23, https://www.bundestag.de/resource/blob/1005444/ed435cb1a5311bb688385a81f295c8a3/WD-7-104-23-pdf.pdf) festhält, verfügt eine Vielzahl von EU-Mitgliedstaaten, u.a. Frankreich, Österreich und die Niederlande über (gesetzliche) Rahmenbedingungen, um das Risiko einer strafrechtlichen Verfolgung mindestens zu minimieren. So berücksichtigt z.B. die niederländische Staatsanwaltschaft, ob ein sog. „Coordinated Vulnerability Disclosure“-Prozess befolgt wurde und misst festgehaltenen grundlegenden Leitlinien (u.a. Verhältnismäßigkeit, Erfordernis der Subsidiarität, usw.) großes Gewicht bei. Aber auch Länder wie die USA und Großbritannien haben bereits Maßnahmen getroffen. Die Bundesregierung sollte endlich einen Reformvorschlag vorlegen, sodass die rechtlichen Rahmenbedingungen in Deutschland modernisiert und damit an internationale Standards angepasst werden können.

Der derzeitig gültige Rechtsrahmen schafft nur Unsicherheiten und Abschreckungseffekte gegenüber talentierten Fachkräften. Durch eine präzise und klar formulierte Gesetzesänderung, die legitime Sicherheitsforschung von kriminellen Aktivitäten unterscheidet, könnte endlich Rechtssicherheit für Sicherheitsforschende gewährleistet

werden. Dies könnte zudem förderliche Auswirkungen auf den Forschungsstandort Deutschland sowie auf das Vertrauen der Bevölkerung in digitale Technologien haben.