GESELLSCHAFT
FÜR INFORMATIK

Berlin, 11. Dezember 2024

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

zur Modernisierung des Computerstrafrechts

Für eine wirksame und zeitgemäße IT-Sicherheitsforschung in Deutschland ist es essenziell, dass das Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren legal durchführbar ist.

Die Gesellschaft für Informatik e.V. (GI) begrüßt es daher ausdrücklich, dass mit dem „Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts“ nun endlich eine tatbestandsausschließende Regelung im deutschen Computerstrafrecht geschaffen wird, die IT-Sicherheitsforscher*innen mehr Rechtssicherheit bei der Ausübung ihres Berufs verspricht. Um die Praxistauglichkeit der angestrebten Regelung zu erzielen, wären jedoch weitere Präzisierungen hilfreich.

§ 202a Abs. 3 StGB-E: Probleme im Nachweis in der Praxis

Der Entwurf verlangt von IT-Sicherheitsforscher*innen den Nachweis, dass ihr Handeln zur Verbesserung der Cybersicherheit dient, ohne jedoch klarzustellen, wie dieser Nachweis zu erbringen ist. Forschende werden daher in der Praxis vor der Herausforderung stehen, Unklarheit darüber zu haben, wie sie ihre Absichten rechtssicher dokumentieren können. In vielen Fällen dürfte die Absicht nicht „unbefugt“ zu handeln, auch künftig nur schwer nachweisbar sein.

Regelungen oder best practices, wie sich Absichten rechtssicher dokumentieren lassen, würden daher die Arbeit der IT-Sicherheitsforscher*innen erheblich erleichtern.

§ 202a Abs. 4 StGB-E: Zeitgemäße Anpassung des Strafrahmens

Die Einführung des Absatz 4 zu schweren Fällen begrüßt die GI. Mit der Erhöhung des Strafmaßes wird der hohen Bedrohungslage bzw. dem Umstand Rechnung getragen, dass die Schäden durch entsprechende Straftaten Versorgungsengpässe, hohe

wirtschaftliche Schäden herbeiführen sowie die Funktionsfähigkeit demokratischer Institutionen beeinträchtigen können.

§ 202c StGB-E: Präzisierung der Unbefugtheit in Vorbereitungshandlungen

Der Gesetzentwurf sieht keine Änderung des sogenannten Hackerparagrafen § 202c StGB vor, da nicht die objektive Eignung von Computerprogrammen zur Tatbegehung entscheidend ist, sondern die Absicht zur Begehung von Straftaten. Dabei ergeben sich jedoch dieselben Herausforderungen wie bei dem Begriff „unbefugt“ in § 202a Abs. 3 StGB-E, da es an verlässlichen Kriterien fehlt, die das Fehlen der „Unbefugtheit“ belegen können.

Insbesondere vor der eigentlichen Ausspähung und dem Abfangen von Daten dürfte die fehlende Unbefugtheit oft nur schwer nachweisbar sein. Vorbereitungshandlungen zur IT-Sicherheitsforschung sollten daher im Wortlaut des §202c klar adressiert werden, um Unklarheiten in der Auslegung entgegen zu wirken.

Zusammenfassung

Die Änderungen gehen eindeutig in die richtige Richtung. Es steht allerdings zu befürchten, dass die Forschenden in der Praxis noch vor einer großen Herausforderung stehen, ihre Absicht nicht unbefugt zu handeln, zu dokumentieren. Präzisierungen im Gesetzestext und entsprechende best practices für Lauterkeitsnachweise könnten die Situation der Forschenden weiter verbessern und damit die IT-Sicherheit Deutschlands stärken.

Über die Gesellschaft für Informatik e.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.