bitkom

Stellungnahme

März 2025

Modernisierung des Computerstrafrechts

Einordnung

Das BMJ hat im November 2024 einen Entwurf zur Modernisierung des Computerstrafrechts vorgelegt. Dieser sollte die Zielsetzung aus dem Koalitionsvertrag 2021 – das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren rechtssicher zu ermöglichen – umsetzen und dabei die Erkenntnisse aus den Symposien zum Reformbedarf im Computerstrafrecht berücksichtigen.

Der Gesetzgeber hat im Zuge der Verabschiedung des 41. Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität im Jahr 2007 versäumt, klare Regelungen zur Rechtmäßigkeit von IT-Sicherheitsforschung zu schaffen. Vertreter der IT-Branche hatten bereits auf die Unsicherheit hingewiesen, die durch die breite Auslegung des sogenannten „Hackerparagraphen“ entsteht, und forderten konkretisierte Erlaubnistatbestände. In Reaktion auf diese Unklarheiten musste das Bundesverfassungsgericht in seinem Beschluss vom 18. Mai 2009 klärende Worte finden. Es stellte fest, dass das „Tatobjekt des § 202c Abs. 1 Nr. 2 StGB nur ein Programm sein kann, dessen Zweck die Begehung einer Straftat nach § 202a StGB (Ausspähen von Daten) oder § 202b StGB (Abfangen von Daten) ist.“ Nichtsdestotrotz bleibt für diejenigen, die Dual-Use-Programme zur Schwachstellenanalyse einsetzen, weiterhin das Risiko bestehen, sich strafbar zu machen, wenn sie nicht ausreichend dokumentieren, dass ihr Handeln den subjektiven Tatbestand erfüllt.

Der Bitkom begrüßt Initiativen zur Entkriminalisierung von IT-Sicherheitsforschenden ausdrücklich. Die Einführung einer tatbestandsausschließenden Regelung stellt einen wichtigen Fortschritt dar, der im Sinne unserer Mitglieder die Rechtssicherheit für die IT-Sicherheitsforschung erhöht. Die bisherigen Regelungen, die auf den Rechtswidrigkeits- oder Schuldausschluss abzielten, hatten sich in der Praxis als wenig praktikabel erwiesen und führten eher zu Unsicherheiten.

Mit dem Bruch der Ampelkoalition wurde die Modernisierung des Computerstrafrechts nicht mehr in den parlamentarischen Prozess eingebracht. Der Entwurf unterliegt damit dem Diskontinuitätsprinzip. Umso wichtiger ist es, die Initiative unter der neuen

Bundesregierung zeitnah wieder aufzugreifen und fortzuführen. Dafür sollte die Zielsetzung für rechtssichere Verfahren zum Identifizieren und Melden von Sicherheitslücken wieder in den neuen Koalitionsvertrag aufgenommen werden. Die nun entstandene Unterbrechung bietet zudem die Gelegenheit, weitere Verbesserungen an dem Entwurf vorzunehmen. Auf diese Weise kann eine Regelung geschaffen werden, die sowohl der IT-Sicherheitsforschung als auch der Cybersicherheit insgesamt zugutekommt.

Allgemeine Anmerkungen

Der Entwurf schafft eine stärkere rechtliche Grundlage für die Sicherheitsforschung, lässt jedoch weiterhin wichtige Fragen zur allgemeinen Rechtssicherheit offen. Auch Definitionen für verantwortungsbewusste Meldungen bleiben unklar. Die komplexen Sachverhalte und Interpretationsspielräume des Gesetzes führen dazu, dass Unternehmen, die im Bereich der Cybersicherheitsforschung tätig sind, nach wie vor mit erheblichen rechtlichen Unsicherheiten konfrontiert werden. Dies betrifft nicht nur die unmittelbar aktiven Unternehmen, sondern hat auch Auswirkungen auf die gesamte Digitalbranche.

Ein zentrales Beispiel für diese Unklarheiten ist die Abgrenzung der Begriffe „Schwachstelle“ und „Sicherheitslücke“ im neuen § 202a Abs. 3 StGB-E. Der Entwurf stellt beide Begriffe nebeneinander, ohne sie systematisch zu definieren. Dies birgt das Risiko, dass eine Schwachstelle als rein technische Sicherheitslücke interpretiert wird, was zu Missverständnissen führen kann. Eine solche Unschärfe wurde bereits im Entwurf des BSI-Gesetzes festgestellt, jedoch ohne klarstellende Definition übernommen. Um Rechtsklarheit zu schaffen und Missverständnisse zu vermeiden, sollte hier eine präzisere Begriffsbestimmung erfolgen.

Eng damit verknüpft ist die Frage der verantwortungsvollen Informationsweitergabe an betroffene Akteure. Der Entwurf sieht in § 202a Abs. 1 StGB-E lediglich eine alternative Information des BSI „oder“ der Verantwortlichen, Hersteller oder Dienstleister vor. In der Praxis ist es jedoch essenziell, dass eine systematische Informationspflicht dieser Akteure verankert wird, damit Schwachstellen schnellstmöglich erkannt und behoben werden können. Verzögerungen, die durch Wartezeiten bei Benachrichtigungen vom BSI entstehen könnten, sollten vermieden werden. Ein solcher Rahmen sollte sich an bewährte internationale Standards wie beispielsweise ISO 29147 anlehnen.

Darüber hinaus sollte die Möglichkeit geschaffen werden, Sicherheitslücken nicht nur an das BSI, sondern auch an weitere relevante Behörden und Aufsichtsstellen zu melden. Neben den Betreibenden und Herstellenden könnten insbesondere die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie die Landesdatenschutzbeauftragten und weitere Stellen auf Bundes-, Landes- oder Kommunalebene einbezogen werden. Dies würde bestehende Meldewege ergänzen.

Schließlich bleibt auch der Schutz von Geschäftsgeheimnissen und Urheberrechten im Kontext der Sicherheitsforschung unzureichend geregelt. Während die Entwurfsbegründung diese Themen anspricht, fehlt eine klare gesetzliche

Absicherung, die verhindert, dass Cybersicherheitsforschung unbeabsichtigt kriminalisiert wird. Insbesondere beim Reverse Engineering wäre eine explizite Regelung notwendig, um Forschenden Rechtssicherheit zu geben, wenn sie schützenswerte Technologien analysieren, ohne sich strafrechtlichen Risiken auszusetzen.

Rechtliche Herausforderungen für Sicherheitsforschende

Grundsätzlich werden mit dem aktuellen Referentenentwurf zur Modernisierung des Computerstrafrechts wichtige Ansätze zur Verbesserung der Rechtssituation für Sicherheitsforschende vorgenommen. Insbesondere die vorgesehenen Voraussetzungen für Straffreiheit, wie die Absicht, „eine Sicherheitslücke festzustellen“, die Meldung der Lücke an Herstellende, Betreibende oder das BSI sowie die technische Erforderlichkeit des Vorgehens zur Feststellung der Lücke, setzen klare Rahmenbedingungen für die Cybersicherheitsforschung.

Sicherheitsforschende wären jedoch trotz der vorgeschlagenen Anpassungen weiterhin rechtlichen Unsicherheiten ausgesetzt. Dies ergibt sich unter anderem aus dem Charakter von nationaler Gesetzgebung, die keine rechtliche Klarheit für Sicherheitsforschung im europäischen Kontext bietet. So bleibt es unklar, welche Konsequenzen es hätte, wenn ein Sicherheitsforscher Tests in einem anderen EU-Mitgliedstaat durchführt. Daher sollte perspektivisch eine einheitliche Regelung auf Unionsebene angestrebt werden, um grenzüberschreitende Sicherheitsforschung rechtlich abzusichern.

Im Detail besteht durch den aktuellen Entwurf weiterhin die Herausforderung, dass Sicherheitsforschende gerichtliche Nachweise für ihre Absichten zur Verbesserung der Cybersicherheit erbringen müssen, ohne dass klare Kriterien festgelegt sind, wie dies geschehen soll. Sowohl in § 202c StGB als auch in § 202a Abs. 3 StGB-E fehlen verlässliche Maßstäbe, um „Unbefugtheit“ nachvollziehbar und rechtssicher zu belegen, insbesondere bei Vorbereitungshandlungen zur Cybersicherheitsforschung. Da Absichten in der Praxis häufig nicht ausreichend nach außen hin erkennbar sind, besteht die Gefahr, dass das Handeln von Sicherheitsforschenden als „unbefugt“ eingestuft wird, was zu rechtlichen Unsicherheiten und potenziellen Konflikten führt. Der Gesetzgeber sollte daher den Wortlaut dieser Vorschriften präziser und transparenter gestalten, um Strafbarkeitslücken zu schließen und Sicherheitsforschenden eine rechtssichere Dokumentation ihrer Absichten zu ermöglichen.

Grundsätzlich wird auch diskutiert, ob zur Adressierung der „Unbefugtheit“ eine Präregistrierung von geplanten Studien, einschließlich einer entsprechenden Risikoabschätzung, in Betracht gezogen werden könnte. Hierfür wäre die Einrichtung einer zentralen Meldestelle beim BSI erforderlich. Dies würde den Vorteil bieten, bereits im Vorfeld die gutwillige Absicht der Forschenden nachzuweisen. Es ist jedoch zu berücksichtigen, dass dieser Ansatz in Teilen der Sicherheitsforschung umstritten ist. Zudem bleibt die grundsätzliche Problematik bestehen, da auch Akteure mit schädlichen Absichten eine Registrierung nutzen könnten, um sich abzusichern oder

gewonnene Informationen weiterzugeben. Schließlich ist fraglich, inwieweit eine fundierte Risikoabschätzung im Vorfeld realistisch möglich ist, da dies oft detaillierte Systemkenntnisse erfordert, die zu Beginn einer Untersuchung noch nicht vorliegen.

Ein weiteres ungelöstes Problem ist, dass es infolge von Anzeigen zu Hausdurchsuchungen kommt, bei denen sämtliche IT-Geräte beschlagnahmt werden. Diese Maßnahmen werden oft durchgeführt, bevor die Intention der Sicherheitsforschenden überhaupt gerichtlich geprüft wird. Auch bei einer positiven Auslegung des Gesetzes bleibt die Möglichkeit von monatelangen oder gar jahrelangen Beschlagnahmungen von IT-Hardware und eine jahrelange Rechtsunsicherheit bestehen– bevor es schließlich zu einem Freispruch kommt. Diese Praxis ist nicht nur eine erhebliche Belastung für die betroffenen Forschenden, sondern gefährdet auch die allgemeine Bereitschaft, im Sinne der allgemeinen Cybersicherheit tätig zu werden und potenzielle Sicherheitslücken zu offenbaren.

Anpassung des rechtlichen Rahmens für Penetrationstests in KRITIS-Umgebungen

Im vorliegenden Entwurf fehlen zentrale Regelungen, die Penetrationstests in kritischen Infrastrukturen unter realistischen Bedingungen ermöglichen, ohne dabei die Betriebssicherheit zu gefährden. Dies ist jedoch essenziell, um Sicherheitslücken frühzeitig zu identifizieren und den Schutz vor Cyberangriffen zu gewährleisten.

Ein zentrales Element ist die Schaffung eines rechtlichen Sonderstatuts für KRITIS-Penetrationstests, das sowohl die besonderen Anforderungen an die Verfügbarkeit als auch an die Betriebssicherheit berücksichtigt. In diesem Zusammenhang sollten in Abstimmung mit dem BSI sogenannte „Safe Testing Windows“ definiert werden, um sicherzustellen, dass sicherheitskritische Prüfungen außerhalb wesentlicher Versorgungszeiten erfolgen. Darüber hinaus sollte ein Fast-Track-Verfahren für die Genehmigung solcher Tests eingeführt werden, um unnötige Verzögerungen zu vermeiden und sicherzustellen, dass zeitkritische Sicherheitsüberprüfungen ohne langwierige Abstimmungsprozesse durchgeführt werden können.

Neben der rechtlichen Absicherung von Penetrationstests muss auch die Haftungsfrage geklärt werden. Die Einführung einer Haftungsobergrenze für unbeabsichtigte Störungen während genehmigter Tests würde sowohl Prüfer als auch KRITIS-Betreiber vor unverhältnismäßigen Risiken schützen. Ergänzend sollten Schutzklauseln für Ausfallzeiten vorgesehen werden, die trotz sorgfältiger Planung auftreten können. Ohne diese Regelungen besteht die Gefahr, dass dringend benötigte Sicherheitsprüfungen unterbleiben, weil die Beteiligten unkalkulierbare Haftungsrisiken fürchten.

Ein weiterer Aspekt ist die Berücksichtigung der gesamten Lieferkette. Die zunehmende Vernetzung kritischer Infrastrukturen macht es notwendig, auch Lieferketten-bezogene Systeme, Cloud-Dienste und externe Dienstleister in Sicherheitstests einzubeziehen. Eine explizite Erlaubnis zur Überprüfung dieser Systeme sowie eine klare gesetzliche Grundlage für die Sicherheitsbewertung von Backup- und Notfallsystemen, einschließlich physischer Sicherheitskomponenten, sind

dringend erforderlich. Angriffe auf kritische Infrastrukturen erfolgen zunehmend hybrid, sodass digitale und physische Sicherheitsmaßnahmen nicht mehr isoliert betrachtet werden können.

Schließlich sollte eine KRITIS-spezifische Zertifizierung für Penetrationstester eingeführt werden, um einen rechtssicheren Qualifikationsnachweis zu schaffen. Dies würde dazu beitragen, einheitliche Standards für Sicherheitstests in kritischen Infrastrukturen zu etablieren und das Vertrauen in die Testergebnisse zu stärken.

Unklarheiten im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)

Ein Aspekt, der im vorliegenden Referentenentwurf leider nicht berücksichtigt wurde, ist die Tatsache, dass IT-Sicherheitsforschung auch unentdeckte Funkdatenabflüsse melden wollen, die möglicherweise auf ein größeres Problem hinweisen – ohne dass eine vollständige root-cause Analyse durchgeführt wurde. Hier steht der § 5 TDDDG der Meldung an eine zuständige Behörde im Weg. Das Abhörverbot, das im TDDDG verankert ist, stammt aus einer Zeit, als wirksame Verschlüsselungsgeräte im Bereich von Funkübertragungen äußerst voluminös waren. Der Stand der Technik hat sich jedoch erheblich weiterentwickelt. Bei Funkkommunikation in sensiblen Bereichen – wie etwa in kritischen Infrastrukturen, im Staats- und Verwaltungsbereich oder bei unverschlüsselten personenbezogenen Daten – ist verschlüsselte Kommunikation mittlerweile die Norm. Dort, wo noch immer unverschlüsselt über Funk kommuniziert wird, stellt dies einen Anlass zur Besorgnis dar und sollte einer staatlichen Prüfung unterzogen werden.

Aufgedeckte Sicherheitslücken in Energieerzeugungsanlagen und andere kritische Infrastrukturanlagen, die eine Steuerung über unverschlüsselte und nicht authentifizierte Funkkommunikation ermöglichen, verdeutlichen das Problem, dass der Staat aktuell nicht ausreichend in der Lage ist, diese Risiken zu prüfen. Zwar werden in manchen sensiblen Bereichen, insbesondere für privatwirtschaftliche Betreiber von KRITIS, Sicherheitsstandards für Funkkommunikation festgelegt, in staatlichen Einrichtungen fehlen jedoch oftmals Vorgaben für Mindestsicherheitsstandards im Bereich der IT-Sicherheit. Der Empfang und die Kenntnisnahme solcher unverschlüsselten Kommunikation, mit dem Zweck, diese an die zuständigen Behörden zu melden, muss daher dringend legalisiert werden. Ein möglicher Ansatz wäre, eine entsprechende Regelung nach dem Wesensgehalt des neuen § 202a (3) StGB zu schaffen, die als neuer § 5 (4) TDDDG implementiert werden könnte.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Bereichsleiter Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Informationssicherheit