VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zum Referentenentwurf des Bundesministeriums der Justiz für ein Gesetz zur Änderung des Strafgesetzbuches zur Modernisierung des Computerstrafrechts

Berlin, 11. Dezember 2024

In den vergangenen Jahren gab es im Rahmen der Digitalisierung einen verstärkten Fokus auf Datenschutz und Informationssicherheit. Nicht zuletzt haben europäische Vorgaben wie die NIS2-Richtlinie hier neue Verpflichtungen eingeführt. Um diesen Verpflichtungen nachzukommen, benötigt die IT-Sicherheitsbranche die Unterstützung der Politik. Trotz einer Stärkung des Fokus auf die Schließung von Sicherheitslücken sind viele etablierte Methoden zur Entdeckung von Schwachstellen und Sicherheitslücken nach der aktuellen Fassung des Strafgesetzbuchs (StGB) strafbewehrt. Mit dem vom Bundesministerium der Justiz (BMJ) am 5.11.2024 vorgelegten Referentenentwurf sollen diese Probleme gelöst und aktuell strafbare Eingriffe in und Angriffe auf Sicherheitssysteme legalisiert werden, wenn sie der IT-Sicherheitsforschung dienen und helfen sollen, Sicherheitslücken zum Zwecke der Schließung zu finden. Gleichzeitig soll das Strafmaß für weiterhin strafbare Eingriffe erhöht werden, um dem gestiegenen Schadensrisiko bei Verletzungshandlungen gerecht zu werden.

Besonders die genauere Differenzierung von erlaubten und unerlaubten Handlungen ist aus Sicht der Internetwirtschaft positiv zu bewerten, um die hier vielfach bestehende Rechtsunsicherheit in der Branche zu beseitigen.

eco – Verband der Internetwirtschaft e.V. hat folgende Anmerkungen zum vorliegenden Referentenentwurf:

- **Zu §202a Absatz 3 StGB: Erlaubte Handlungen**

Der an den § 202a StGB neu angefügte Absatz 3 benennt zwei Voraussetzungen, unter denen der unbefugte Zugriff auf gesicherte Daten nach den Absätzen 1 und 2 nicht strafbar ist. Demnach sind entsprechende Maßnahmen erlaubt, wenn diese eine Sicherheitslücke in einem System aufdecken und die für die Schließung zuständige Stelle informiert werden soll. Ferner muss die Maßnahme für das Aufdecken der Sicherheitslücke erforderlich sein.

Da die vorgeschlagenen Regelungen in großen Teilen der bereits angewendeten Praxis im Bereich der IT-Sicherheit entsprechen, begrüßen wir diese Klarstellung im Gesetzestext. Das Eindringen in bzw. „Hacken" von Systemen, um Schwachstellen aufzudecken, ist eine der wenigen praktischen Möglichkeiten der IT-Sicherheitsforschung. Diese ist nicht nur in Zeiten zunehmender Digitalisierung immer wichtiger geworden. Selbst europäische Richtlinien wie die NIS2-Richtlinie, die mehr Maßnahmen zur IT-Sicherheit von Kritischer Infrastruktur und

Unternehmen fordert, empfiehlt explizit das systematische Aufdecken von Sicherheitslücken, um entsprechende Schwachstellen zu beheben, bevor es zu tatsächlichen Angriffen kommt. In einer Zeit, in der effektive Sicherheitssysteme nicht nur für die Integrität essenziell wichtig, sondern auch gesetzlich vorgeschrieben sind, ist es von besonderer Bedeutung, dass der Gesetzgeber jegliche Rechtsunsicherheit vermeidet. Dabei ist auch zu beachten, dass die Adressaten der Regelung oft keine oder nur eine geringe juristische Ausbildung haben. Daher ist es sehr zu begrüßen, dass die neue Regelung die Voraussetzungen klar formuliert, sodass auch für juristisch nicht geschultes Personal leicht erkennbar ist, welche Maßnahmen erlaubt sind, und welche weiterhin strafbar sind.

- **Zu §202a Absatz 4 StGB: Erhöhtes Strafmaß für besonders schwere Fälle**

Absatz 4 des Entwurfs sieht ein erhöhtes Strafmaß in besonders schweren Fällen vor. Zur Feststellung, wann ein besonders schwerer Fall vorliegt, nennt Absatz 4 drei mögliche Kriterien. Demnach liegt ein besonders schwerer Fall vor, wenn der Angriff bei dem Betroffenen einen großen finanziellen Schaden verursacht, der Täter gewerbsmäßig oder als Teil einer organisierten Bande handelt, oder der Angriff die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer Kritischen Infrastruktur, der Bundesrepublik Deutschland oder eines Bundeslands beeinträchtigt.

Auch diese Änderungen sind zu begrüßen. Mit der Ausformulierung reagiert der Gesetzgeber auf die neu entstandenen Risiken. Während Nummer 2 eine Reaktion auf zunehmende Angriffe von organisierten Gruppen darstellt, greift Nummer 3 die besondere Stellung von Kritischer Infrastruktur auf. Zusätzlich wird dadurch die Differenzierung von schädlichen Angriffen zu den nach Absatz 3 straffreien Angriffen weiter hervorgehoben. Auch wenn diese Regelung weder bestehende Sicherheitsmaßnahmen verstärkt noch bei der Behebung von entstandenen Schäden hilft, so hat sie doch Potenzial für eine zunehmend abschreckende Wirkung.

- **Zu §202b Absatz 2 und §303a Absatz 4 StGB: Weitere Anwendungsfälle**

Der neu geschaffene Absatz 2 in §202b StGB sieht die Anwendung sowohl der Ausnahmen als auch des erhöhten Strafmaßes für Fälle des Abfangens von Daten vor. Parallel dazu sieht der neue Absatz 4 in §303a des Entwurfs lediglich die Anwendung der Ausnahmen im Falle der Datenveränderung vor. Wie bereits zuvor ausgeführt, ist auch diese neue Ausprägung zu begrüßen. Sowohl das Abfangen als auch das Verändern von Daten sind Tatbestände, die regelmäßig bei der systematischen Aufdeckung von Schwachstellen erfüllt werden. Entsprechend ist es nur konsequent, die zu diesem Zwecke dienlichen Ausnahmen bei allen im Zuge dessen auftretenden Fällen anzuwenden und ausdrücklich zu erwähnen. Dies erleichtert technisch versierten, jedoch juristisch fachfremden Adressaten der Normen die Einschätzung über die potenzielle Strafbarkeit.

Fazit

Die vorgesehenen Anpassungen des Computerstrafrechts sind aus Sicht des eco ein Schritt in die richtige Richtung. In Zeiten, in denen sich auch immer mehr Aspekte des öffentlichen Lebens im digitalen Raum abspielen, ist es wichtig, dass dieser entsprechend geschützt ist. Um einen solchen Schutz zu ermöglichen, müssen die entsprechende Personen, die die Sicherheit von IT-Systemen verbessern wollen, in jederlei Hinsicht unterstützt werden. Genau dazu dienen die neuen Regelungen, um IT-Sicherheitsexperten nicht nur vor Strafbarkeit zu schützen, sondern ihnen im Gegenzug Rückhalt durch den Gesetzgeber zu geben. Die Ausnahmen der Strafbarkeit schützen nicht nur vor Strafverfolgung, sondern ermutigen sogar dazu, Sicherheitslücken durch praxisnahe Methoden und Angriffe aufzudecken und daraufhin zu schließen. Damit folgt der Gesetzgeber auch der Empfehlung der Europäischen Union, die genau diese Methode für die IT-Sicherheitsbranche empfiehlt. Gleichzeitig reagiert das Einführen von besonders schweren Fällen auf das mit dem digitalen Fokus einhergehenden erhöhten Sicherheitsrisiko. Das für diese Fälle vorgesehene erhöhte Strafmaß ist grundsätzlich ebenfalls begrüßenswert, allerdings ist dies nur dann hilfreich, wenn solche Angriffe auch aufgeklärt werden können. Um hier einen vollumfänglich effektiven Schutz zu ermöglichen ist der vorliegende Entwurf also ein guter Ansatz, allein jedoch nicht voll ausreichend. Eine Möglichkeit, den Ansatz konsequenter zu verfolgen, ist ein Verweis in § 202c StGB auf die neu eingeführten Ausnahmen. Auch wenn ein solcher Verweis laut Gesetzgeber nicht notwendig sei, da die neuen Regelungen nach gängiger Rechtsprechung bereits für § 202c StGB gelten würden, wäre ein expliziter Verweis dennoch hilfreich für die von der Norm betroffenen juristisch fachfremden Adressaten.