November 2024

Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts

- Informationspapier -

Computerstrafrecht sanktioniert Straftaten, die im Zusammenhang mit Computern und der digitalen Welt stehen. Mit dem Entwurf zur Modernisierung des Computerstrafrechts schlägt das BMJ zwei Anpassungen vor. (1) Es soll ein **Tatbestandsausschluss für bestimmte Handlungen von IT-Sicherheitsforschern** geschaffen werden. So soll gesetzlich klargestellt werden, dass bestimmte Handlungen von IT-Sicherheitsforschern nicht nach dem Computerstrafrecht bestraft werden können; konkret geht es dabei um die Schwachstellenforschung, aber auch die Tätigkeit von IT-Sicherheitsunternehmen sowie von sog. „Hackern", wenn sie in der Absicht handeln Sicherheitslücken aufzuspüren und zu schließen. (2) Außerdem soll das **Strafrecht für bestimmte Fälle des Ausspähens von Daten verschärft** werden.

Zur Vorbereitung des Entwurfs hat das Bundesjustizministerium im vergangenen Jahr zwei Symposien durchgeführt. Bei diesen Symposien wurde umfassend untersucht, inwieweit das geltende Computerstrafrecht aufgrund der fortschreitenden technischen Entwicklung reformbedürftig ist. An den Symposien haben Expertinnen und Experten aus der Wissenschaft und der Praxis (Strafverfolgung, Anwaltschaft, IT-Sicherheitsforschung) sowie Vertreterinnen und Vertreter der Landesjustizverwaltungen, des Bundesinnenministeriums und des Bundesamtes für Sicherheit in der Informationstechnik teilgenommen. Die dort gewonnen Erkenntnisse haben gezeigt, dass es - über die vorgeschlagenen Änderungen hinaus - aktuell keinen grundlegenden Reformbedarf im Computerstrafrecht gibt.

I. Tatbestandsausschluss für bestimmte Handlungen von IT-Sicherheitsforschern

Warum besteht gesetzgeberischer Handlungsbedarf?

Durch die zunehmende Komplexität von IT-Systemen und die teilweise schwachen Sicherheitseinstellungen von IT-Produkten, können Sicherheitslücken in IT-Systemen entstehen. Das Aufspüren dieser Sicherheitslücken gehört zu den typischen Tätigkeiten der IT-Sicherheitsforschung, von IT-Sicherheitsunternehmen, die Penetrationstests anbieten, oder von Hackern, die sich zum Ziel gesetzt haben, IT-Sicherheitslücken zu finden und zu schließen. Dafür muss jedoch häufig auf fremde Systeme und Daten zugegriffen werden, die sich bereits im praktischen Einsatz befinden. Dies birgt Strafbarkeitsrisiken für die IT-Sicherheitsforschung. Dies kann sich kontraproduktiv auswirken, weil diese Risiken nicht nur von verbotenem, sondern auch von gesellschaftlich erwünschtem Verhalten abschrecken. IT-Sicherheit ist die „Achillesferse" der modernen Gesellschaft. Sie können von Cyberkriminellen, aber auch von fremden Mächten (z. B. Russland) ausgenutzt werden und zu großen gesellschaftlichen Schäden führen (Bsp.: Krankenhäuser oder Verkehrsunternehmen, die Energiewirtschaft, Verwaltungsbehörden können erpresst und lahmgelegt werden, wenn Kriminelle sich Zugang zu ihren System verschaffen). Die Aufdeckung und Schließung von Sicherheitslücken ist daher im gesamtgesellschaftlichen Interesse. Diese Strafbarkeitsrisiken für die IT-Sicherheitsforschung sollen ausgeschlossen werden.

Welche Änderungen im Strafgesetzbuch schlägt das Bundesjustizministerium vor, um Strafbarkeitsrisiken für die IT-Sicherheitsforschung zu vermeiden?

Die vorgeschlagene Änderung betrifft in erster Linie den Straftatbestand des Ausspähens von Daten (§ 202a Strafgesetzbuch (StGB)). Nach dieser Strafnorm macht sich strafbar, wer sich „unbefugt" Zugang zu Daten verschafft. Durch eine Ergänzung der Norm soll klar geregelt werden, unter welchen Umständen es *nicht* „unbefugt" und damit *nicht* strafbar ist, sich Zugang zu Daten zu verschaffen. Dafür

soll ein neuer Absatz 3 in die Vorschrift aufgenommen werden. Der dadurch neu geregelte Strafbarkeitsausschluss soll auch für zwei weitere Straftatbestände gelten: das Abfangen von Daten (§202b StGB) und die Datenveränderung (§ 303a StGB). In diesen Normen soll zukünftig auf den neuen § 202a Abs. 3 StGB verwiesen werden.

An welche Voraussetzungen soll der neue Strafbarkeitsausschluss geknüpft sein?

In dem neuen § 202a Abs. 3 StGB soll geregelt sein, dass eine Handlung dann *nicht* „unbefugt" und damit *nicht* strafbar ist, wenn folgende Voraussetzungen *kumulativ* erfüllt sind:

- Die Handlung ist in der Absicht erfolgt, eine Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems (Sicherheitslücke) festzustellen (**Feststellungsabsicht**).
- Die Handlung ist in der Absicht erfolgt, die Information über eine festgestellte Sicherheitslücke gegebenenfalls an eine verantwortliche Stelle weiterzugeben, die in der Lage ist, die Lücke zu schließen oder dies zu veranlassen (**Unterrichtungsabsicht**). Das sind die für das informationstechnische System Verantwortlichen, der betreibenden Dienstleister des jeweiligen Systems, der Hersteller der betroffenen IT-Anwendung *oder* das Bundesamt für Sicherheit in der Informationstechnik (BSI).
- Die Handlung ist zur Feststellung der Sicherheitslücke erforderlich (**Erforderlichkeit**).

Unter welchen Voraussetzungen besteht die Absicht, eine Schwachstelle festzustellen und darüber zu unterrichten?

Eine Feststellungsabsicht wird nicht anzunehmen sein, wenn die betreffende Person mutwilligen ausprobiert, ob sich Systeme „knacken" lassen - und dabei nicht den Plan verfolgt, eine etwaig festgestellte Schwachstelle gegebenenfalls auch zu melden. Das Gesetz schreibt allerdings keine feste Meldemethode vor; dafür gibt es auch noch kein anerkanntes, standardisiertes Verfahren (responsible disclosure). Es soll nicht ausreichen, wenn die betreffende Person lediglich in der Absicht handelt, die Lücke einfach irgendjemandem mitzuteilen oder sie öffentlich zu machen. Die beabsichtigte Meldung muss an einen Verantwortlichen gerichtet sein, der in der Lage ist, die Lücke zu schließen oder dies zu veranlassen, oder aber an das BSI.

Wann ist eine Handlung „erforderlich" (§ 202a Abs. 3 Nr. 2)?

Die Regelung schafft keinen „Freibrief", sich auf einem IT-System nach Belieben umzusehen. Ein Strafbarkeitsausschluss soll lediglich dann greifen, wenn die Handlung zur Feststellung der Sicherheitslücke erforderlich ist. Dadurch soll sichergestellt werden, dass keine Strafbarkeitslücken entstehen. Wer auf mehr oder andere Daten zugreift, als dies für die Feststellung der Sicherheitslücke notwendig ist, soll sich weiterhin strafbar machen.

Warum wird nicht auch der „Hackerparagraph" § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten) geändert?

Die Änderungen der §§ 202a und 202b StGB werden dazu führen, dass für die IT-Sicherheitsforschung keine Strafbarkeitsrisiken mehr bestehen. Eine Änderung des § 202c StGB ist nicht notwendig. Das Bundesverfassungsgericht hat hier Klarheit geschafft; dies wird in der Begründung ausführlich dargelegt. Die Vorschrift des § 202c StGB setzt nämlich voraus, dass das Tatobjekt ein Computerprogramm ist, dessen Zweck die Begehung einer Tat nach § 202a oder § 202b StGB ist. Ferner muss der Täter eine Straftat nach den §§ 202a und 202b StGB vorbereiten. Selbst wenn ein „Hackertool" zu kriminellen Zwecken hergestellt und verbreitet wurde, kann jedermann sich dieses Tool straffrei verschaffen, wenn es zur IT-Sicherheitsforschung benötigt wird.

II. Normierung weiterer besonders schwere Fälle des Ausspähens + Abfangens von Daten

Welche Anpassungen am geltenden Recht schlägt das Bundesjustizministerium vor?

Die Strafvorschriften des Ausspähens von Daten (§ 202a StGB) und des Abfangens von Daten (§ 202b StGB) sollen ergänzt werden um Regelungen für besonders schwere Fälle. Entsprechende Fälle des Ausspähens von Daten und des Abfangens von Daten sollen strenger bestraft werden als bislang. Der Strafrahmen für diese Fälle soll auf Freiheitsstrafe von drei Monaten bis zu fünf Jahren erhöhen lauten.

Ein solcher besonders schwerer Fall soll in der Regel vorliegen, wenn der Täter einen Vermögensverlust großen Ausmaßes herbeiführt (§ 202a Abs. 5 Nr. 1 StGB) oder aus Gewinnsucht, gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Taten nach den §§ 202a, 202b StGB verbunden hat (202a Abs. 5 Nr. 2 StGB). Außerdem sollen die Fälle erfasst werden, in denen – auch aus dem Ausland – durch die Tat die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer kritischen Infrastruktur oder die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder beeinträchtigt wird (§ 202a Abs. 5 Nr. 3 StGB).

Warum besteht hier gesetzgeberischer Handlungsbedarf?

Nach dem geltenden Recht kann das Ausspähen von Daten mit Freiheitsstrafe bis zu drei Jahren bestraft werden, das Abfangen von Daten mit Freiheitsstrafen bis zu zwei Jahren. Für die besonders schweren Fälle des Ausspähens und des Abfangens von Daten ist dieser Strafrahmen nicht angemessen. Solche Computerdelikte können ein erhebliches Schadenspotential (z. B. wenn kritische Infrastruktur betroffen ist) und einen erheblichen Unrechtsgehalt haben.