CyberStR

ZEITSCHRIFT FÜR CYBERSTRAFRECHT

DATA | TECH | CRIME | MEDIA

Heft 1 · Juli 2025
Seiten 1 – 54
1. Jahrgang
ISSN 3052-5926
Art. Nr. 60252501

Carl Heymanns Verlag

1|2025

Pro: »Strafrecht für IT-Sicherheitsforschung entschärfen – Grey Hat Hacking legalisieren«

Dr. Eren Basar, Düsseldorf

1986 hat der deutsche Gesetzgeber § 202a StGB eingeführt und damit das »Ausspähen von Daten« als Zentralnorm des deutschen »Hacking-Strafrechts« unter Strafe gestellt. Bis auf die – deklaratorische – Erstreckung des Wortlauts von § 202a StGB auf das Verschaffen des unbefugten Datenzugangs im Jahr 2007 ist dieses Gesetz trotz der gewandelten IT-Sicherheitslage bis heute unverändert geblieben. Der Gesetzgeber hält damit 2025 daran fest, dass das Aufspüren von Sicherheitslücken in informationstechnischen Systemen eines Unternehmens mittels invasiver Testmethoden nur straffrei sein soll, *»soweit der ›Hacker‹ vom Inhaber des Unternehmens mit dieser Aufgabe betraut wurde«* (BT-Drucks. 16/3656, 10).

Das gegebenenfalls tadellose Motiv eines der IT-Sicherheit verbundenen Hackers kann danach an der Strafbarkeit der unbeauftragten Sicherheitsforschung nichts ändern. Der sog. *Grey-Hat-Hacker* kann stattdessen nur hoffen, dass der von ihm gegebenenfalls einer IT-Schwachstelle Überführte auf den grundsätzlich erforderlichen Strafantrag (vgl. § 205 StGB) verzichtet. Lässt der Betroffene keine Nachsicht walten, bleibt ihm nur das Vertrauen in die Milde der Strafjustiz – ein Umstand, der keine Rechtssicherheit vermittelt. Bislang wenig Beachtung findet, dass die in Unternehmen tätigen IT-Security Teams ebenfalls mit dem Risiko der Strafbarkeit konfrontiert sind, wenn sie Tests durchführen. Das Einverständnis des Arbeitgebers erweist sich oft als unzureichend, um die strafrechtliche Relevanz von Penetrationstests auszuschließen. Die Vernetzung der unternehmenseigenen IT-Systeme mit externen Cloud-Dienstleistern führt dazu, dass diese Tests zwangsläufig Auswirkungen auf Systeme haben, die außerhalb der unmittelbaren Kontrolle des Unternehmens liegen.

Externe Dienstleister zeigen häufig wenig Interesse daran, fremden Teams die Durchführung solcher Tests zu gestatten, da dies möglicherweise mit eigenen Sicherheitsrisiken verbunden ist. Die ursprünglich vom Gesetzgeber vorgesehene Lösung für Grey-Hat-Hacker, die auf der Einverständniserklärung des Unternehmens basierte, ist durch diese Entwicklungen damit überholt.

Das passt nicht mehr: Auch das Strafrecht darf nicht ignorieren, dass die IT-Sicherheitslage aufgrund zunehmender Angriffe so angespannt ist wie nie zuvor. Diese Risikosituation wird durch die fortschreitende Komplexität von Programmen und Systemen verschärft, die Schwachstellen nahezu unvermeidbar macht. Das BSI berichtet für 2023 von durchschnittlich 78 neuen Schwachstellen täglich. Unternehmen sehen sich einer Flut von sanktionsbewehrten IT-sicherheitsrechtlichen Regelwerken, vor allem aus Europa, gegenüber. Angesichts dieser Lage darf das Strafrecht nicht dazu beitragen, die gemeinschaftliche IT-Sicherheit durch undifferenzierte Strafbarkeit sicherheitsfördernder Handlungen zu untergraben. Stattdessen sollte das Strafrecht Grenzen setzen, um unkoordinierte Eingriffe unter dem Deckmantel der IT-Sicherheitsforschung zu verhindern. Ein umfassendes Verbot ist jedoch das falsche Instrument.

Der Entwurf des Bundesjustizministeriums zur Modernisierung des Computerstrafrechts von 2024 verdient daher Zustimmung. Die Schaffung eines speziellen Rechtsfertigungsgrundes zur Entschärfung der Strafbarkeitszone für Grey-Hat-Hacking ist der richtige Weg, um die Balance zwischen den Interessen der Allgemeinheit, des Hackers und des Betroffenen zu erreichen. Fragen bleiben jedoch offen: Wann wird eine sicherheitsbezogene Maßnahme strafwürdig, weil sie überwiegend schädigend oder als illegitime Bevormundung des IT-sicherheitsrechtlich Verantwortlichen eingestuft wird? Der Vorschlag des Ministeriums besteht darin, diesen Konflikt durch eine Befugnisnorm zu lösen, die subjektiv die Absicht, eine Sicherheitslücke zu erkennen und zu melden, und objektiv deren »Erforderlichkeit« voraussetzt. Diese strafrechtliche Würdigung der »IT-Sicherheit« ist längst überfällig, doch bleibt fraglich, ob das Strafbarkeitsrisiko für IT-Sicherheitsforschung damit hinreichend reduziert würde. Insbesondere berücksichtigt die Regelung nicht das typische Vorgehen bei Penetrationstests, die nicht auf eine bestimmte Sicherheitslücke abzielen, sondern das Gesamtsystem auf Schwächen prüfen.

Der neue Koalitionsvertrag 2025 äußert sich nicht eindeutig zur Entschärfung der Strafbarkeit des Grey Hat Hacking. Das Versprechen »Rechtssicherheit für IT-Sicherheitsforschung zu schaffen und Missbrauch zu verhindern« bleibt vage. Gleichwohl zeigt die Diskussion um den Reformvorschlag des Bundesjustizministeriums die dringende Notwendigkeit einer Reform auf. Ansonsten bliebe die Rechtslage paradox: Einerseits erfordern Regulierungen von Unternehmen, die Informationssicherheit umfassend zu gewährleisten, andererseits ist das Strafrecht so strukturiert, dass beinahe jeder Sicherheitstest ein Strafbarkeitsrisiko darstellt. Es ist an der Zeit, diesen Widerspruch aufzulösen.

Contra: »Strafrecht für IT-Sicherheitsforschung entschärfen – Grey Hat Hacking legalisieren«

Jana Ringwald, Frankfurt

Cybercrime-Bekämpfung ist eine Sisyphusarbeit. Sie ist technisch aufwendig, erfordert ein datenverständnisorientiertes Arbeiten, das nicht Teil der DNA von Strafverfolgungsbehörden ist und muss oft ohne das Leitplankensystem des BGH auskommen, weil so häufig rechtliches Neuland betreten wird. Bei all dem können wir eins nicht gebrauchen: die Verfolgung von Taten, die in der Gesellschaft gewünscht sind. Das Aufspüren von IT-Sicherheitslücken ist dafür ein Kandidat.

Der Grey Hat Hacker ist kein Black Hat Hacker. Er ist aber auch kein White Hat Hacker. Mit anderen Worten: er geht weder kriminell vor, noch mit Erlaubnis. Die vorgebliche Intention von Netzaktivisten ist es, IT-Systeme sicherer zu machen. Allerdings handeln Grey Hat Hacker in der Regel nicht mit dem Einverständnis der »Getesteten« und nutzen mitunter fragwürdige Methoden. Allerdings kann es auch wünschenswert sein, in natürlichen Umgebungen Sicherheitslücken aufzuspüren, ohne zuvor ein Einverständnis einzuholen. Es gilt also genauer hinzuschauen.

Das Aufspüren von Sicherheitslücken in IT-Systemen darf nicht strafbar sein, wenn es sozialadäquates oder sogar gemeinnütziges Verhalten darstellt. Aber ist es sozialadäquat, nicht nur der wissenschaftlichen Forschung, sondern auch der unabhängigen IT-Sicherheitsforschung, bzw. Netzaktivisten Straffreiheit zu garantieren? Bei der Antwort hilft der Blick in die Gesellschaft.

Dort stellen wir fest, dass Unternehmen und Institutionen, deren Sicherheitslücken Grey Hat Hacker festgestellt haben, durchaus Strafanzeige erstatten. Obwohl sie unstreitig auf eine eigene Sicherheitslücke hingewiesen wurden und daran ein hohes Interesse haben sollten. Wie genau es zu dieser Erkenntnis kommt, scheint also für die Betroffenen relevant zu sein. Deswegen darf dieser Umstand nicht nassforsch mit dem alleinigen Argument, die IT-Landschaft absichern zu wollen, abgetan werden. Bei solchen »Angriffen« erlangen Grey Hat Hacker regelmäßig Daten, die das betroffene Unternehmen nicht in fremden Händen wissen will. Von einer uneingeschränkten Sozialadäquanz des Grey Hacking können wir daher nicht ausgehen.

Grey Hat Hacker suchen sich aktuell aus, wen sie »pen-testen« und wen nicht. Darunter befinden sich auch privat betriebene Computersysteme. Dass deren Sicherheitslücken eine tatsächliche Gefahr für die IT-Sicherheit und den Datenschutz im größeren, gesetzlich zu schützenden Rahmen bergen, wäre wohl eine Übertreibung.

Dass es bei all dem um den Schutz von Unternehmen und Institutionen gehen soll, gibt auch der Gesetzgeber in seinem Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches im Sinne der Modernisierung des Computerstrafrechts zu erkennen. So verweist die Gesetzesbegründung ausdrücklich auf die Resolution der Generalversammlung der Vereinten Nationen vom 25.09.2015 und deren Nachhaltigkeitsziels 9 – den Aufbau einer widerstandsfähigen Infrastruktur. Auch der Verweis des Entwurfs auf die NIS-2-Richtlinie, nach der Schwachstellen häufig von Dritten entdeckt werden, und die eine koordinierte Offenlegung von Schwachstellen empfiehlt, richtet den Fokus auf Unternehmen und Institutionen.

Sollen die sich nun entspannen, weil der Referentenentwurf für ein straffreies Hacking auch die Absicht fordert, Betroffene über die festgestellte Sicherheitslücke zu unterrichten? Dann ist doch alles in Butter! Bislang existiert aber kein anerkanntes Standardverfahren zur Meldung von IT-Sicherheitslücken (sog. *»responsible disclosure«*). Ohne klare Vorgaben zur Meldung von Sicherheitslücken besteht für die Betroffenen die Gefahr erpresserischen Verhaltens der »Angreifer«. Denn Täter können ohne Weiteres neben ihren Feststellungs- und Unterrichtungsabsichten Schädigungsabsichten verfolgen. Etwa wenn nach der Feststellung eine Ausnutzung der Schwachstelle erfolgt, um sodann das Unternehmen über das Bestehen der Sicherheitslücke zu informieren. Es darf aber nur straffrei bleiben, was *ausschließlich* in der Absicht erfolgt, eine Schwachstelle oder ein anderes Sicherheitsrisiko festzustellen. Ebenso ist die Absicht einer *unverzüglichen* Unterrichtung der Verantwortlichen zu fordern.

Die Schließung von Sicherheitslücken hat allergrößte Bedeutung für die Abwehr von Cyberangriffen. Unternehmen und Institutionen müssen das zweifellos konstruktive Aufspüren ihrer Sicherheitslücken nicht nur hinnehmen, sondern begrüßen. Dies wird ihnen leichter fallen, sobald ein Standardmeldeverfahren etabliert ist. Unbeauftragtes »Pen-testing« privat betriebener Systeme kann gleichwohl nicht als gesellschaftlicher Konsens angesehen werden und sollte von einer Straffreiheit ausgenommen werden. Grey Hat Hacker dürfen nur straffrei bleiben, wenn sie sich nachweislich wie White Hat Hacker aufführen. Wenn Netzaktivisten entscheiden dürfen, wen sie testen und wie sie dabei vorgehen, darf kein Zweifel bleiben, ob sie sich wirklich in den Dienst der Sache stellen. Wenn dies Gesetz wird, haben sie noch einen Grund, den grauen gegen den weißen Hut zu tauschen.