Aktuelle Reformbestrebungen zu § 202a StGB

Der dritte Tatkomplex (Strafbarkeit des A wegen des Aufdeckens der Sicherheitslücke) in Fall 11 beschäftigt sich mit dem sog. White Hat-Hacking, also Hackern, die ihre technischen Fähigkeiten dafür einsetzen, Sicherheitslücken aufzudecken, um die IT-Sicherheit in Deutschland zu erhöhen. Wie Sie bereits aus der Lösung zu Fall 11 ersehen können, ist es höchst problematisch, ob Hacking auch dann strafbar ist bzw. sein soll, wenn der Hacker nur deshalb in das System eindringt, weil er eine etwaige Sicherheitslücke aufdecken und dem betroffenen Unternehmen und/oder dem Bundesamt für Sicherheit in der Informationstechnik (BSI) melden will. Das Bundesjustizministerium hat Anfang November 2024 – damals noch unter dem Justizminister a.D. Dr. Marco Buschmann – deshalb einen Referentenentwurf vorgelegt, wonach Hacking dann straflos sein soll, wenn der Täter in der Absicht handelt, IT-Sicherheitslücken aufzudecken und das Hacking auch für die Aufdeckung der IT-Sicherheitslücke erforderlich ist. Neben anderen Änderungen sollte dem § 202a StGB ein dritter Absatz angefügt werden:

„Die Handlung ist nicht unbefugt im Sinne des Absatzes 1, wenn

1. sie in der Absicht erfolgt, eine Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems (Sicherheitslücke) festzustellen und die für das informationstechnische System Verantwortlichen, den betreibenden Dienstleister des jeweiligen Systems, den Hersteller der betroffenen IT-Anwendung oder das Bundesamt für Sicherheit in der Informationstechnik über die festgestellte Sicherheitslücke zu unterrichten und

2. sie zur Feststellung der Sicherheitslücke erforderlich ist."[1]

Diese Regelung wäre auf den dritten Tatkomplex von Fall 11 anwendbar, mit der Folge, dass A bereits nach dieser Regelung straflos wäre. Denn angesichts der Tatsache, dass A die Systeme von X nur deshalb untersucht, weil er von deren Problemen in der IT-Sicherheit gehört hat und diese aufdecken will, handelt A mit der im neuen Absatz 3 vorausgesetzten Absicht zur Feststellung einer Sicherheitslücke. Aufgrund der späteren Meldung ist davon auszugehen, dass A auch bereits bei der Tathandlung ebenfalls die Absicht verfolgte, diese Sicherheitslücke an X zu melden. Auch die Entwurfsverfasser gehen davon aus, dass die notwendige Absicht durch das Tatgericht stets anhand objektiver Merkmale zu bestimmen sein wird und man sich nicht nur auf eine entsprechende Behauptung des Angeklagten verlassen könne.[2] Weiterhin wäre das Handeln des A nach der in der Lösung vertretenen Auffassung auch „erforderlich", da kein gleich effektives, aber milderes Mittel zur Aufdeckung vorhanden war (a.A. wie in der Lösung geschildert allerdings vertretbar) und auch eine etwaige Interessenabwägung (Verhältnismäßigkeit ieS) zugunsten des A ausgeht (für Details, siehe Lösung zu Fall 11 im Buch).

Würde eine solche Regelung also in Kraft treten, ließen sich viele der derzeit problematischen Fälle des White Hat-Hackings hierüber lösen. Da jedoch bei Abfassung des hiesigen Textes (am 21.11.2024) unwahrscheinlich ist, dass der Referentenentwurf noch in der derzeitigen Legislaturperiode verabschiedet wird, ist unklar, ob eine solche Regelung jemals umgesetzt wird. Mit Hilfe des QR-Codes im Buch können Sie bei dieser hochaktuellen rechtpolitischen

[1] Abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_ComputerStrafR.pdf?__blob=publicationFile&v=3 (Stand: 21.11.2024).
[2] Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Moder-nisierung des Computerstrafrechts, S. 8.

Frage stets auf dem Laufenden bleiben. Wenn es Neuigkeiten hierzu gibt, können Sie diese jeweils hier nachlesen.