Mehr Rechtssicherheit für die Cybersicherheitsforschung! [Editorial]

Annika Selzer, Benedikt Buchner

Angaben zur Veröffentlichung / Publication details:

Selzer, Annika, and Benedikt Buchner. 2024. "Mehr Rechtssicherheit für die Cybersicherheitsforschung! [Editorial]." Datenschutz und Datensicherheit - DuD 48 (12): 765. https://doi.org/10.1007/s11623-024-2013-z.

Mehr Rechtssicherheit für die Cybersicherheitsforschung!

Um den aktuellen Stand der Cybersicherheit zu analysieren, müssen Cybersicherheitsforschende häufig die Rolle böswilliger Angreifer simulieren. Auf diese Weise können sie neue Cyberangriffsmethoden besser verstehen und für die den Angriffen zugrunde liegenden Schwachstellen Gegenmaßnahmen ableiten. Hierdurch werden wiederum nicht nur die IT und die mittels IT verarbeiteten Daten, sondern auch die Gesellschaft als solche vor den Auswirkungen von Cyberangriffen geschützt. Obwohl die Cybersicherheitsforschung vor diesem Hintergrund also an sich einen hohen Stellenwert einnimmt, sieht sie sich erheblichen rechtlichen Problemen gegenüber: Bestehende Gesetze, die auf die einzelnen Forschungsaktivitäten im Bereich der Cybersicherheitsforschung Anwendung finden, stellen häufig einen großen Unsicherheitsfaktor dar, weil diese „allgemeingültig" sind, also nicht speziell den Bereich der Cybersicherheitsforschung normieren und somit auch nicht die Besonderheiten der Cybersicherheitsforschung mitberücksichtigen. Im Ergebnis bewegt sich die Cybersicherheitsforschung in weiten Teilen in einer rechtlichen Grauzone, was wiederum mittel- bis langfristig dazu führen kann, dass Cybersicherheitsforschungsaktivitäten aus Angst vor Strafen nicht (mehr) durchgeführt werden und somit die Cybersicherheit nicht aufrechterhalten werden kann (s. dazu schon *Selzer/Stummer/Boll*, ATHENE-Positionspapier, 2024; *Selzer/Spiecker gen. Döhmann*, Tagesspiegel Background, 2022).

Diesem Problem möchte sich die vorliegende Ausgabe mit dem Schwerpunkt „Rechtrahmen der Cybersicherheitsforschung" im Rahmen von fünf Schwerpunktbeiträgen annehmen. *Kriegel et al.* stellen in ihrem Beitrag die Ergebnisse einer Simulationsstudie vor, in deren Rahmen ein Simulationsgericht über die strafrechtliche Relevanz von Aktivitäten der Cybersicherheitsforschung befunden hat. Die Simulationsstudie wurde Ende September 2024 vom Nationalen Forschungszentrum für angewandte Cybersicherheitsforschung ATHENE mit einem Strafrichter, einem Staatsanwalt und zwei Strafverteidigern durchgeführt und soll in den kommenden Jahren fortgesetzt werden. Im Beitrag von *Botes* werden ethische und rechtliche Aspekte der Cybersicherheitsforschung im Bereich der fortgeschrittenen Mensch-Computer-Schnittstellen diskutiert. Thema des Beitrags von *Gärtner* ist die aktive Cyberabwehr; verschiedene Maßnahmen der aktiven Cyberabwehr werden benannt und so kategorisiert, dass eine Betrachtung der rechtlichen Zulässigkeit dieser Maßnahmen (in der Cybersicherheitsforschung) überhaupt erst möglich wird. Der Beitrag von *Appelt* plädiert dafür, innerhalb der offensiven Cybersicherheitsforschung die Anforderungen an Datenschutz und Cybersicherheit bereits im Implementierungsprozess neuer Tools zur Abwehr von Cyberangriffen zu berücksichtigen und unterbreitet hierfür einen praxisorientierten Vorschlag. *Schreiber et al.* schließlich beleuchten in ihrem Good-Practice-Beitrag die Offenlegung von Cybersicherheitsschwachstellen aus technischer Sicht.

Wir hoffen, mit dieser Themenzusammenstellung die Diskussion rund um den Rechtsrahmen der Cybersicherheitsforschung weiter vorantreiben und einen Anstoß geben zu können, die dringend benötigte Rechtssicherheit für die Cybersicherheitsforschung als Grundlage einer starken Cybersicherheit, aber auch eines starken Datenschutzes weiterzuverfolgen.

Annika Selzer und Benedikt Buchner