Cybersicherheitsforschung

Annika Selzer, Benedikt Buchner

Angaben zur Veröffentlichung / Publication details:

Selzer, Annika, and Benedikt Buchner. 2024. “Cybersicherheitsforschung.” Datenschutz und Datensicherheit - DuD 48 (12): 814. https://doi.org/10.1007/s11623-024-2024-9.

Annika Selzer, Benedikt Buchner

Cybersicherheitsforschung

1 Ein Wettlauf gegen die Zeit

Neuartige IT-Schwachstellen und -Angriffsmethoden fordern die Cybersicherheit immer wieder heraus. Für ein hohes Maß an Cybersicherheit ist hierbei entscheidend, wer den Wettlauf um die Identifizierung neuer Schwachstellen und Angriffsmethoden gewinnt: Sind es böswillige Angreifer, die die identifizierten Schwachstellen und Angriffsmethoden umgehend für Angriffe auf Behörden, Unternehmen oder Privatpersonen ausnutzen? Oder sind es Cybersicherheitsforschende, die sogleich versuchen, die im Rahmen ihrer Forschung identifizierten Schwachstellen an relevante Stellen zu melden, damit die Schwachstellen schnellstmöglich behoben werden können, oder aber selbst Schutzmaßnahmen gegen neue Angriffsmethoden ableiten?[1]

Damit Cybersicherheitsforschende diesen Wettlauf gewinnen und somit für ein hohes Maß an Cybersicherheit sorgen können, muss es ihnen möglich sein, agil und gewissermaßen „kreativ" zu arbeiten. Denn nicht selten müssen Cybersicherheitsforschende im Rahmen ihrer Arbeit die große Leistung vollbringen, sich in böswillige Angreifer hineinzuversetzen, um – teilweise unter großem Zeitdruck – unter anderem

- in einer Testumgebung die gleichen Methoden und Werkzeuge wie diese zu benutzen, um neuartige Angriffe besser verstehen zu können, Gegenmaßnahmen ableiten zu können und diese Gegenmaßnahmen bei akut stattfindenden, realen Angriffen anwenden zu können;
- das Ausmaß und bereits entstandene Schäden neuartiger Angriffe – unter anderen durch Recherchen im Darknet – zu identifizieren und
- durch Sicherheitstests Schutzlücken frühzeitig zu identifizieren und zu ermitteln, wie viele Rechner/Personen/Einrichtungen von einer Schutzlücke potenziell betroffen sein könnten.

Die stetig zunehmenden Bedrohungen für die Cybersicherheit lassen sich bereits heute oftmals nur mittels o.g. Vorgehensweisen begegnen und es ist zu erwarten, dass die Bedeutung dieser Vorgehensweisen in den kommenden Jahren – unter anderem aufgrund der ansteigenden Automatisierbarkeit von Cybersicherheitsangriffen – weiter anwachsen wird.[2]

2 Rechtsunsicherheit als Hemmschuh

Dass Cybersicherheitsforschende im Rahmen dieser Arbeiten nicht nur ethische Grundsätze und Anforderungen an die Wissenschaftlichkeit ihrer Arbeiten, sondern auch den für ihre Forschung geltenden Rechtsrahmen beachten müssen, versteht sich von selbst. Die Beachtung dieser Grundsätze und Anforderungen sind zentrale Voraussetzungen für Forschungsergebnisse, die den gesellschaftlichen Schutz und Nutzen in den Fokus ihrer Untersuchungen rücken.[3]

Jedoch ist das im Rahmen der Cybersicherheitsforschung geltende Recht immer wieder ein Unsicherheitsfaktor für die Forschenden. Zum einen liegt das daran, dass die für ihre Forschung geltenden Rechtsakte häufig veraltet sind und somit dem technischen Fortschritt hinterherhinken. Zum anderen sind die einschlägigen Rechtsakte in der Regel nicht mit der Zielsetzung entstanden, speziell den Bereich der Cybersicherheitsforschung zu regeln, und gehen somit nicht speziell auf die Gegebenheiten der Cybersicherheitsforschung ein. Für Cybersicherheitsforschende ist damit aber nicht klar erkennbar, welche der grundsätzlich zielführenden Forschungsarbeiten rechtskonform sind, welche in einem rechtlichen Graubereich liegen oder welche gar rechtswidrig sind.[4]

3 Höhere Rechtssicherheit führt zu höherem gesellschaftlichem Schutz

Die Rechtsunsicherheit in der Cybersicherheitsforschung geht so weit, dass Cybersicherheitsforschende auch hohe Geldbußen oder sogar Haftstrafen befürchten müssten. Dieser Umstand wird sich wiederum mittel- bis langfristig negativ auf das Cybersicherheitsniveau auswirken. Denn wenn Cybersicherheitsforschende im Rahmen ihrer Arbeit nicht sicher sein können, ob und wann sie geltendes Recht verletzen, besteht das Risiko, dass die dringend benötigte Agilität und Kreativität im Rahmen der Erforschung von Abhilfemaßnahmen gegen neuartige Bedrohungen verloren gehen.[5]

Eine starke Forschungslandschaft ist jedoch Grundvoraussetzung für ein hohes Maß an Cybersicherheit. Davon wiederum profitiert letztlich die gesamte Gesellschaft, sei es, weil Angriffe gegen Anbieter Kritischer Infrastrukturen abgewehrt werden, der Abgriff geistigen und gewerblichen Eigentums aus unseren Unternehmen verhindert oder das Ausspionieren natürlicher Personen unterbunden wird. Cybersicherheitsforschung geht uns alle an!

1 Die diesem Beitrag zugrundeliegenden Forschungsarbeiten wurden vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der Beitrag gibt die persönliche Meinung der Autoren wieder.

2 Boll, DuD 2023, S. 346; Gärtner/Selzer, Tagesspiegel Background, 2022; Selzer/Spiecker gen. Döhmann/Boll, DuD 2023, S. 785 f.

3 Selzer/Spiecker gen. Döhmann, Tagesspiegel Background, 2022.

4 Mit konkreten Beispielen: Selzer/Spiecker gen. Döhmann, Tagesspiegel Background, 2022.

5 Selzer/Stummer/Boll, Positionspapier zur 2. DSGVO Evaluation, 2024, S. 3.