ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Mein Code, dein Code, unser Code?
Cybersicherheitsforschung und das Urheberrecht

Prof. Dr. Gerald Spindler
Mit einem technischen Problemaufriss von Dr. Steven Arzt

Kurzzusammenfassung des gleichnamigen Vortrags im Rahmen der Veranstaltungsreihe „Rechtsrahmen der Cybersicherheitsforschung“

veranstaltet von Dr. Annika Selzer und Prof. Dr. Indra Spiecker geb. Döhmann

Impressum

Layout und Satz
Jasmin Bastian

Kontakt
Nationales Forschungszentrum für angewandte
Cybersicherheit ATHENE
c/o Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

Hinweise

Dieser Beitrag wurde 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.

Cybersicherheitsforschung und das Urheberrecht

Ein technischer Problemaufriss von Dr. Steven Arzt

In der Softwaresicherheit entwickeln IT-Sicherheitsforschende neue Methoden zur Feststellung des Sicherheitsniveaus von Software. Man unterscheidet dabei grundsätzlich zwischen statischen und dynamischen Verfahren:

- Dynamische Verfahren beobachten eine Software zur Laufzeit und ziehen hieraus Rückschlüsse über das Sicherheitsniveau der Software.
- Statische Verfahren betrachten den Binär- oder Quellcode einer Software, um Rückschlüsse über deren Sicherheitsniveau zu ziehen.

Um neuartige Verfahren zur Überprüfung des Sicherheitsniveaus von Sofware wissenschaftlich evaluieren zu können, ist eine Auswertung auf einer großen Anzahl von Softwareartefakten notwendig. Diese werden oftmals aus Repositories bezogen, wie beispielsweise aus den App-Stores der großen Mobilanbieter. In diesem Zusammenhang ergeben sich für IT-Sicherheitsforschende zahlreiche Fragen im Bereich des Urheberrechts.[1] Beispielsweise ist unklar, welche Aktionen bzw. welche Verfahren der statischen Analyse von Software bereits einer Disassemblierung und Dekompilierung[2] gleichkommen.

Hierbei ist darauf zu verweisen, dass für eine statistische Aussage über neue Verfahren zur Überprüfung des Sicherheitsniveaus von Software i.d.R. eine Massenevaluation von Software notwendig ist. Häufig werden hunderte oder sogar tausende Programmdateien unterschiedlicher Hersteller und/oder Privatpersonen, die diese in die jeweiligen App-Stores eingebracht haben, analysiert. Eine einzelne vertragliche Grundlage mit den jeweiligen Urheberrechtsinhabern zu schaffen ist bei einer derartigen Massenevaluation nicht realistisch ist.

Im Ausland wird häufig auf ein Forschungsprivileg verwiesen. Zusätzlich zur hausintern durchgeführten Forschung an der Software kann die Software dort als Datengrundlage zusammen mit den Forschungsdaten, die mittels der neuartigen Verfahren zur Überprüfung des Sicherheitsniveaus von Software aus der jeweils analysierten Software extrahiert wurden, der wissenschaftlichen Gemeinschaft zur Verfügung gestellt werden. Dies ermöglicht anderen Wissenschaftlern, die eigenen Experimente zu reproduzieren, was ohne Zugang zur analysierten Software nicht möglich ist. Dies ist wichtig, um die Ergebnisse unabhängig verifizierbar zu machen. In Deutschland gestaltet sich die Lage mangels eines solchen Forschungsprivilegs leider weit weniger eindeutig. Hier ist es daher wichtig, entsprechende Rechtssicherheit für die Forschenden zu schaffen, beziehungsweise die Grenzen und Möglichkeiten von Softwaresicherheitsforschung in Bezug auf das Urheberrecht herauszuarbeiten.

Dr. Steven Arzt ist Leiter der Abteilung Secure Software Engineering am Fraunhofer-Institut für sichere Informationstechnologie SIT und Koordinator des Forschungsbereichs Automatic Vulnerability Scanning and Verification am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE.

[1] Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe des Urheberrechts.

[2] Mittels Disassemblierung und Dekompilierung wird binärer Programmcode einer Software so umgewandelt, dass er nicht nur von Maschinen, sondern auch von Menschen gelesen werden kann.

Cybersicherheitsforschung und das Urheberrecht

Ein rechtlicher Kurzüberblick von Prof. Dr. Gerald Spindler

Eine Analyse der Software – wie von Dr. Arzt beschrieben – kann urheberrechtlich jenseits von entsprechenden Klauseln in Lizenzverträgen nur durchgeführt werden, wenn nach deutschem (und europäischem) Urheberrecht entsprechende Schranken eingreifen. In Betracht kommen hier nur § 69d UrhG oder die Anwendung von Text- und Datamining-Schranken nach §§ 44b, 60d UrhG bzw. Art. 3, 4 DSM-Richtlinie.[3]

Für Software selbst gelangt indes nur die Schranke des § 69d UrhG zur Anwendung. Eine Dekompilierung ist nach dieser Norm nicht zulässig, sondern nur nach § 69e UrhG zur Herstellung von Interoperabilität. § 69d UrhG beschränkt zudem die Zulässigkeit der Beobachtung und des Testens von Software von vornherein auf denjenigen, der zur Verwendung „eines Vervielfältigungsstücks eines Programms" berechtigt ist. Mithin können etwa nicht beliebig viele Softwareartefakte in einem App-Store durch einen Dritten untersucht werden – dieses Recht bleibt dem Betreiber des App-Stores vorbehalten,[4] außer wenn der untersuchende Dritte selbst das Programm erworben hat. Sofern diese Bedingung vorliegt, kann indes das jeweilige Programm getestet werden, um die ihm zugrundeliegenden „Ideen und Grundsätze" zu ermitteln, wozu auch Aspekte der Cybersicherheit gehören. Dass die Schranke des § 69d Abs. 3 UrhG nur den Kreis der ohnehin Berechtigten betrifft, zeigt zudem der Kreis der erfassten „Handlungen zum Laden, Anzeigen, Ablaufen, Übertragen oder Speichern des Programms". Die Rechtmäßigkeit der technischen Dekompilierung muss hierbei Einzelfall-abhängig bewertet werden. Darüber hinaus gehende Vervielfältigungen bleiben weiterhin unzulässig. Gleiches gilt für die von § 69d Abs. 1 UrhG ermöglichte Fehlerberichtigung bei Programmen: Auch hier kann nur der „Berechigte" die Fehlersuche und -berichtigung vornehmen, nicht aber z.B. generell eine Forschungsinstitution oder ein anderer Dritter.

Auch wenn das Text- und Datamining auf den ersten Blick auch auf Software anwendbar ist, da § 44b Abs. 1 UrhG bzw. § 60d UrhG auf die „… automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken" ausgerichtet ist, „um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen" hat der Gesetzgeber die Anwendung von § 60d UrhG explizit ausgeschlossen nach § 69d Abs. 6 UrhG. Zudem spricht Art. 3 DSM-RL nicht die Rechte nach der Software-Richtlinie an. Unabhängig davon ist allerdings die kommerzielle Auswertung von Software entsprechend Art. 4 Abs. 1 DSM-Richtlinie – sofern der Rechteinhaber dies nicht in maschinenlesbarer Form ausschließt. Möglich bleibt daher nach § 60d UrhG nur das Mining von Daten, die zuvor bereits im Rahmen von Cybersicherheitsuntersuchungen angefallen sind.

Prof. Dr. Gerald Spindler ist Inhaber des Lehrstuhls für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Rechtsvergleichung, Multimedia- und Telekommunikationsrecht und Direktor des Instituts für Wirtschafts- und Medienrecht an der Georg-August-Universität Göttingen.

---

[3] Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG, ABl. L 130/92 vom 17.5.2019

[4] Diesen Ausführungen wird das Fallbeispiel zugrunde gelegt, dass alle App-Hersteller ihre Urheberverwertungsrechte vollständig an den App-Store übertragen haben (unabhängig einer Verrechnung zwischen App-Hersteller und App-Store).

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Mein Code, dein Code, unser Code?
Cybersicherheitsforschung und das Urheberrecht