ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Nur ein paar Gesundheitsdaten? Datenschutz als Nebenschauplatz der Cybersicherheitsforschung

Prof. Dr. Gerrit Hornung
Mit einem technischen Problemaufriss von York Yannikos

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

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

Impressum

Layout und Satz
Olivia Gude

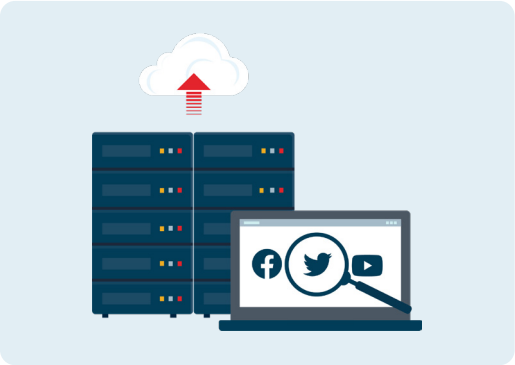
Kontakt
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

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.

Datenschutz in der Cybersicherheitsforschung

Ein technischer Problemaufriss von York Yannikos



IT-Sicherheitsforscher*innen befassen sich unter anderem mit Fragestellungen rund um die Entstehung und Verbreitung von Extremismus und Desinformationen. In entsprechenden Forschungsprojekten wird dazu Open Source Intelligence (kurz: OSINT) eingesetzt. Mittels OSINT werden aus offenen, frei zugänglichen Quellen im Internet Daten gesammelt und zu bestimmten Fragestellungen untersucht. Ein Beispiel für eine solche Fragestellung ist, ob sich Hasskommentare oder Fake News automatisiert erkennen lassen können. Als Datenquellen der wissenschaftlichen Untersuchungen kommen soziale Netzwerke oder Kommunikationsplattformen wie Facebook, Twitter oder Telegram in Betracht. Auch frei zugängliche Dienste für den Austausch von Videos und Bildern wie YouTube oder Instagram oder auch Diskussionsforen und Chaträume kommen als Datenquellen in Frage.

In den Informationen, die mit OSINT aus diesen Quellen gesammelt werden können, sind sehr oft auch personenbezogene oder personenbeziehbare Daten enthalten – selbst dann, wenn der Name des eigenen Nutzerprofils auf einer solchen Plattform beliebig gewählt werden kann, also gar nicht dem eigentlichen Klarnamen entsprechen muss (dieser frei gewählte Name wird auch als „Pseudonym" bezeichnet). Beispielsweise können Angaben wie der Geburtstag oder Aufenthaltsort dazu beitragen, dass Personen identifizierbar werden. Auch sehr sensible Informationen, z.B. über den Gesundheitszustand einer Person, können mittels OSINT erhoben und analysiert werden. Ob und in welchem Umfang entsprechende Daten mit OSINT erhoben werden, ist nicht immer von vornherein klar. Beim Einsatz von OSINT ist es deshalb wichtig, von Anfang an die Frage zu stellen, wie der Schutz gesammelter personenbezogener und -beziehbarer Daten gewährleistet werden kann, insbesondere, wenn diese Daten

- analysiert,
- an Projektpartner weitergegeben oder
- veröffentlicht werden sollen.

Datenschutz in der Cybersicherheitsforschung

Ein rechtlicher Kurzüberblick von Prof. Dr. Gerrit Hornung

Öffentlich zugängliche Internetinformationen sind eine Fundgrube für private und staatliche Stellen – von der Beobachtung des Images eines Unternehmens über die Gewinnung nachrichtendienstlicher Erkenntnisse bis hin zur sozialwissenschaftlichen Forschung. So legitim diese Ziele im Einzelfall sein können – ihre Verfolgung muss sich im Rahmen des geltenden Datenschutzrechts bewegen. Als zentraler Ausgangspunkt ist festzuhalten, dass die Öffentlichkeit personenbezogener Daten jedenfalls nach deutschem und europäischem Verständnis diese nicht ihres Schutzes beraubt: Grundrecht auf Datenschutz und DSGVO erfassen geheime wie öffentliche personenbezogene Daten. Der Umfang des Schutzes kann allerdings unterschiedlich ausfallen; in der Bestimmung dieser Anforderungen liegt die eigentliche Herausforderung für eine datenschutzkonforme Cybersicherheitsforschung.

Da die Veröffentlichung von Daten im Netz noch keine umfassende Einwilligung in die Nutzung durch Dritte darstellt, richtet sich die Zulässigkeit der Verarbeitung nach einer umfassenden Abwägung – sei es nach Art. 6 I f DSGVO (private Forschungsstellen) oder nach den Verarbeitungsgeneralklauseln für staatliche Universitäten. Im Rahmen der Abwägung ist die grundrechtliche Forschungsfreiheit maßgeblich zu berücksichtigen, kann sich aber nicht in allen Fällen durchsetzen. Insbesondere bei Gesundheits- und anderen sensiblen Daten kann die Abwägung anders ausfallen. Dies gilt v.a., weil Daten auch durch Dritte (und ggf. rechtsmissbräuchlich) im Netz gelandet sein können.

Fragen des Datenschutzes durch Technikgestaltung spielen auch in der Cybersicherheitsforschung eine wichtige Rolle, stoßen aber oftmals an Grenzen. Eine echte Anonymisierung erfordert z.B. nicht nur die Löschung des Accounts eines Posts, sondern auch das Entfernen personenbezogener Daten aus dem Inhalt. Im Rahmen der Weitergabe an Dritte hat das Argument Gewicht, dass diese sich die Daten grds. auch selbst im Netz beschaffen könnten. Allein entscheidend ist dieses jedoch nicht, v.a. wenn es um umfassende Datenbestände und Persönlichkeitsprofile geht. Dementsprechend bedarf es auch hier einer Rechtsgrundlage für die Übermittlung sowie ergänzender technisch-organisatorischer Maßnahmen zum Persönlichkeitsschutz.

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Nur ein paar Gesundheitsdaten? Datenschutz als Nebenschauplatz der Cybersicherheitsforschung