Mehr Rechtssicherheit für die IT-Sicherheitsforschung

Unabhängige IT-Sicherheitsforschung ist ein essentieller Baustein für eine sichere Digitalisierung

Mit der Digitalisierung und Vernetzung wächst die Abhängigkeit unserer Gesellschaft von Informations- und Kommunikationstechnik. IT-Produkte sind trotz größtmöglicher Sorgfalt selten frei von **Sicherheitslücken**. Werden diese spät oder gar nicht entdeckt, können Kriminelle sie ausnutzen. Dadurch entstehen unmittelbar **erhebliche Gefahren für Staat, Gesellschaft und Wirtschaft**. Es wird daher immer wichtiger, Schwachstellen so früh wie möglich zu finden und zu beheben. Folglich besteht auch ein großes **gesamtgesellschaftliches Interesse** an einer starken **IT-Sicherheitsforschung** durch neutrale Stellen, die rechtzeitig Risiken aufzeigen, bevor es zum Schaden kommt.[1]

IT-Sicherheitsforschende sind in Deutschland von Haftungs- und Strafbarkeitsrisiken bedroht

Für die gewissenhafte Durchführung von IT-Sicherheitsuntersuchungen ist in vielen Fällen **Reverse Engineering** notwendig. Dabei wird systematisch die Funktions- und Konstruktionsweise eines unbekannten Systems oder Produkts ermittelt. **Urheberrechtlich** sind einige Formen des Reverse Engineerings ohne Zustimmung der Urheber*innen verboten. Da IT-Systeme in der Regel aus verschiedenen Teilprogrammen unterschiedlicher, weltweit tätiger Hersteller*innen zusammengesetzt sind, ist die Erteilung einer Einwilligung in der Praxis unrealistisch. Bestehende Erlaubnisnormen greifen für die Forschung regelmäßig zu kurz.

Die IT-Sicherheitsforschung muss sich zudem **realistischer Angriffsszenarien und -methoden** bedienen, um neue Sicherheitsmechanismen und Präventionswerkzeuge zu entwickeln und bestehende zu analysieren. Dafür müssen sich Forschende in Bezug auf echte Produkte teils ähnlichen Methoden und technischen Vorgehensweisen bedienen wie Cyberkriminelle. Das aktuelle **IT-Strafrecht** differenziert jedoch nur unzureichend nach den verfolgten Absichten.

Fehlende Erlaubnisnormen für IT-Sicherheitsuntersuchungen im Urheber- und Strafrecht

Forschende in Deutschland werden aufgrund drohender rechtlicher Konsequenzen **abgeschreckt** IT-Sicherheitslücken zu **untersuchen** und an Produktverantwortliche zu **melden**. Da Hochschulen gesetzlich zu wissenschaftlicher Redlichkeit verpflichtet sind, dürfen sie keine Projekte betreiben, wenn diese gegen geltendes Recht verstoßen könnten.

Die **Geheimhaltung von Schwachstellen führt nicht zur Erhöhung der Sicherheit** von Produkten und Systemen. Erfolgversprechend und auch wirtschaftlich nachhaltig ist nur das **Beheben der Fehler** sowie eine **Veröffentlichung der Erkenntnisse** der IT-Sicherheitsforschung. Dabei ist zu bevorzugen, den Produktverantwortlichen erst die Möglichkeit zur Fehlerbehebung zu geben und für einen **überschaubaren Zeitraum** die Veröffentlichung der Forschungsergebnisse aufzuschieben. Die Erfahrung hat gezeigt, dass eine funktionierende **Zusammenarbeit** zur Aufdeckung und Behebung zahlreicher Schwachstellen führt und damit einen wertvollen Beitrag zur nachhaltigen Verbesserung der Sicherheit von Informationssystemen leistet. Daher möchten die Unterzeichnenden sowohl das Bewusstsein für die **Bedeutung der Zusammenarbeit zwischen Hersteller*innen und der IT-Sicherheitscommunity stärken** als auch auf rechtliche Hemmnisse hinweisen.

Eine **erfolgreiche IT-Sicherheitsforschung** trägt nachweislich zur **Erhöhung des Sicherheitsniveaus** von IT-Produkten bei und ist daher von hohem **gesellschaftlichem** und auch **wirtschaftlichem Nutzen**. Daher fordern Forschende für IT-Sicherheit den Gesetzgeber auf, diese **Rechtsunsicherheit zu beseitigen.**

[1] Zu rechtlichen und technischen Hintergründen: Whitepaper zur Rechtslage der IT-Sicherheitsforschung, 2021: https://sec4research.de/.

Empfehlungen

1. Rechtssicherheit für die IT-Sicherheitsforschung

Die derzeitigen urheber- und strafrechtlichen Vorschriften erschweren die Forschungsarbeit, da sie keine klaren Regelungen zugunsten einer **redlich durchgeführten IT-Sicherheitsforschung** beinhalten. Forscher/innen, die sich an etablierte wissenschaftliche und ethische Standards halten, müssen **vor strafrechtlichen Sanktionen sowie zivilrechtlichen Unterlassungs- und Schadensersatzansprüchen effektiv geschützt** werden.

- *Wir fordern den Gesetzgeber dazu auf, die rechtlichen Rahmenbedingungen so zu gestalten, dass redliche IT-Sicherheitsforschung erleichtert und gefördert wird. Sie darf für die Forschenden kein erhebliches Risiko bedeuten, wie es allerdings derzeit aus zu weitreichenden zivil- und strafrechtlichen Regelungen folgt.*

2. Klare Standards für den Umgang mit Sicherheitslücken

Aufbauend auf klaren rechtlichen Rahmenbedingungen empfiehlt sich auch, dass die beteiligten Akteur*innen **klare Standards für den Umgang mit Sicherheitslücken** vereinbaren: Dies ermöglicht es, die Interessen von Wissenschaft, Gesellschaft und Wirtschaft in Einklang zu bringen. Ein international genutzter Mechanismus ist die „Coordinated bzw. Responsible Vulnerablity Disclosure“. Dabei werden Schwachstellen erst den Produktverantwortlichen gemeldet. Nach erfolgreicher Problembehebung oder wenn zu vermuten ist, dass keine Lösung erstellt wird, wird die Öffentlichkeit informiert. Nutzer*innen wird so ermöglicht Schutzmaßnahmen zu ergreifen und Schäden abzuwenden. Dieser Mechanismus ist in Deutschland jedoch noch nicht flächendeckend etabliert und im geltenden Rechtsrahmen nicht verankert.

Ein derartiges kooperatives Vorgehen erfordert gegenseitige Rücksichtnahme sowie klare und verlässliche Zusagen. Einen einheitlichen Rahmen kann ein **Standard der IT-Sicherheitsforschung** liefern, auf den sich die IT-Sicherheitsforschung und die IT-Wirtschaft Deutschlands einigen. Daneben können leicht zugängliche **Anlaufstellen**, die bei der Meldung von Sicherheitslücken unterstützen, die Kommunikation moderieren, Zusammenarbeit fördern und im Zweifel Möglichkeiten zur Konfliktlösung bieten.

- *Wir fordern Forschungseinrichtungen, Unternehmen, Wirtschaftsverbände und die Politik dazu auf, sich gemeinsam für die Etablierung klarer Standards für den Umgang mit IT-Sicherheitslücken einzusetzen.*

3. International eine Vorreiterrolle übernehmen durch klares Bekenntnis zur IT-Sicherheitsforschung

Die Zukunft des Wirtschaftsstandorts Deutschland ist von der **IT-Sicherheit** abhängig. Mit Blick auf den internationalen Wettbewerb führt lokale Rechtsunsicherheit zum **Verlust der Attraktivität des Forschungsstandorts Deutschland**. Andere Länder verfügen bereits über Regeln für redliche IT-Sicherheitsforschung oder arbeiten daran (z.B. Niederlande, USA). Mit einer Reform des Rechtsrahmens schafft Deutschland auch eine Blaupause für internationale Lösungen. Forschungserkenntnisse, welche die Digitalisierung sicherer machen, müssen ihren Weg in die Praxis finden können. Ein offener Austausch zum Forschungsstand ist fester Bestand jeglicher Forschung. Erst mit einem rechtssicheren Rahmen für den Beitrag von akademisch Forschenden, kommerziellen Penetrationstester*innen und IT-Sicherheitsexpert*innen kann Deutschlands Forschungs- und IT-Sicherheitslandschaft mehr **nutzbare Ergebnisse für die Wirtschaft generieren.**

- *Wir regen einen internationalen Dialog an, um die Nutzung sowie rechtliche Verankerung der genannten Kooperationsmechanismen zur Behebung und Offenlegung von Schwachstellen zu fördern. Deutschland sollte sich auch international für eine einheitliche Lösung aktiv einbringen und mitgestalten, um Standortnachteile für IT-Sicherheitsforschende zu beseitigen.*