Prüfsteine Überarbeitung Hackerparagraph - Arbeitsfassung

Die aktuelle Fassung der §§ 202 a - d StGB hat praktisch zur Folge, dass im Bereich der IT ohne Zustimmung und Einflussnahme der Hersteller keine unabhängigen Gutachten zu proprietären Produkten erstellt werden können. Dies hat Auswirkungen sowohl für die Justiz im Rahmen der Beweisführung vor Gericht als auch für den demokratischen Diskurs im Bereich der Berichterstattung. Die aktuellen Diskussionen u.a. um die UN Cybercrime Prevention explizit im Zusammenhang mit dem in Entwicklung befindlichen Cyber Ressilience Act der EU lassen eine Verschlechterung der Situation erwarten.

Eine umfassende legale Untersuchung von Digitalprodukten ist bisher gemäß § 7a Untersuchung der Sicherheit in der Informationstechnik BSI-Gesetz [0], dem BSI unter strengen Auflagen vorbehalten.

Im Rahmen einer Überarbeitung des Hackerparagraphen sind folgende Punkte zu beachten:

- Befähigung von Verbraucherschutz und Verbänden

  Eine der genuinen Aufgaben von Verbraucherschutzorganisationen und Verbänden ist die Produktprüfung für die von Ihnen vertretenen Interessengruppen.
  Für digitale Produkte ist eine unabhängige Prüfung von Produkten weder eigenständig noch durch Beauftragung entsprechender Fachunternehmen möglich.

  Mithin sind Verbraucherschutzorganisationen und Verbände darauf angewiesen, ihrer Arbeit ausschließlich anhand von Herstellerangaben oder in den Medien öffentlich werdenden Informationen nachzukommen. Eine für andere Produkte übliche Unabhängige Prüfung, bspw. Stiftung Warentest, Crashtests von Autos oder berufsüblicher Werkzeuge (Bohrmaschinen, Stethoskope) ist nicht möglich.

  Der 2022 bekannteste Fall ist die Irreführung der Gematik sowie der Öffentlichkeit über die Komplexität eines Software-Updates der Krypto Zertifikate von Konnektoren. Diese wurde durch den Sicherheitsforscher Flüpke des CCC im Oktober 2022 nachgewiesen [1]. Dies hatte zur Folge, dass der mit 300 - 400 Millionen Kosten bezifferte Konnektoren Tausch bei umschwenken der Update Strategie von Hardwaretausch zu Softwareupdate 220 - 320 Millionen Euro sparte [2].

  Mit Einführung der Muster Feststellungsklage fehlt Verbraucherschutzorganisationen und Verbänden weiterhin die Möglichkeit, durch eine unabhängige Prüfung ohne Kenntnis der herstellenden Firma die Erfolgsaussichten eines solchen mit erheblichen Streitwerten beachteten Verfahren außergerichtlich fundiert abzuschätzen.

- Befähigung der Justiz

  Im Bereich der Justiz besteht hier ein erhebliches Verdunklungs Risiko. Im Rahmen des VW Abgasskandals [3] war es dem Hersteller nicht möglich eine Veränderung an der Software vorzunehmen, da die Autos nicht standardmäßig vernetzt waren. Im Rahmen von Cloud Dienstleistungen, die vollständig unter der Kontrolle der Hersteller liegen oder Anwendungen, die kontinuierlich geupdated werden, können ggf. bestehende bekannte täuschende Mängel auch noch nach Klageerhebung unauffällig behoben werden. Aktuell ist bspw. Das Erstellen von unabhängigen Gutachten, die bereits Klageeinreichungen beigelegt werden, können nicht möglich.

- Ermöglichung unabhängiger Sicherheitsforschung

  Im August 2022 hat der Sicherheitsforscher Martin Tschirsich wiederholt nachgewiesen, dass das bis dahin gängige Video Ident Verfahren mit einfachen technischen Mittel überwunden werden kann [4]. Ein erster Beweis wurde 2018 von Jan Garcia vorgestellt [5] Hiermit bestätigte beide die Existenz der Sicherheitsmängel auf die Hochschule Bonn-Rhein-Sieg 2017 [6], das BSI im Lagebericht 2018 [7] und der BfDI im Tätigkeitsbericht 2020 [8] hingewiesen hatten.

  In beiden Fällen war die Dokumentation der Sicherheits Forschenden hinreichend vage gehalten, um diese nicht gerichtsfest verklagen zu können. Auf eine solche gerichtsfeste Dokumentation von Vorfällen wären aber bspw. Verbraucherschutzorganisationen und Verbände angewiesen.

- Überprüfung Auslieferungsabkommen

  Auch wenn in der deutschen Rechtsgeschichte trotz wiederholter Anzeigen, bspw. von Lilith Wittmann durch die CDU [9] und anderen Fällen [10] noch keine Sicherheitsforscher*in rechtskräftig verurteilt wurde, ist dies im Ausland nicht der Fall [11]. Entsprechend ergibt sich aus der weiten Fassung des §§ 202 im Rahmen üblicher Auslieferungsabkommen für Sicherheitsforscher*innen in Deutschland das Risiko einer Auslieferung und Verurteilung. Explizit, da aufgrund zusehends vernetzter Systeme bei der Untersuchung eines Systems einer deutschen Firma ein Subsystem eines ausländischen Dienstleisters betroffen sein kann. Ein Beispiel hierfür stellen die Sicherheitsvorfälle des US-Dienstleisters Ivanti dar [12] welche in 12 norwegischen Ministerien eingesetzt wurde [13].

  Im internationalen Vergleich existieren auch positive Beispiele, beispielsweise in Belgien [14].

Quellen:

[0] https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
[1] ccc.de/de/updates/2022/konnektoren-400-millionen-geschenk
[2] sueddeutsche.de/wirtschaft/konnektoren-zahnaerzte-anzeige-1.5734874
[3] https://de.wikipedia.org/wiki/Abgasskandal
[4] https://www.ccc.de/de/updates/2022/chaos-computer-club-hackt-video-ident
[5] https://media.ccc.de/v/35c3-9616-circumventing_video_identification_using_augmented_reality
[6] S.22: https://www.h-brs.de/sites/default/files/brs_18_01_jahresbericht_2017_rz10_web.pdf
[7] S.22 1.3.5 Identitätsmissbrauch durch Fernidentifizierungsverfahren https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3
[8] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/29TB_20.html
[9] https://www.sueddeutsche.de/politik/cdu-connect-anzeige-wittmann-1.5373488
[10] https://www.heise.de/news/Modern-Solution-Anklage-gegen-Aufdecker-von-Sicherheitsluecke-gescheitert-9182813.html
[11] https://timesofmalta.com/articles/view/we-wanted-help-students-arrested-exposing-freehour-security-flaw.1024757
[12] https://www.heise.de/news/Ivanti-schliesst-Zero-Day-Luecke-in-MobileIron-9225583.html
[13] https://www.golem.de/news/zero-day-luecke-ausgenutzt-hacker-stehlen-daten-von-12-norwegischen-ministerien-2307-176137.html
[14] https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/