PARTEI DES FORTSCHRITTS

PDF

Positionspapier: Hackerparagraph

Positionspapier: Hackerparagraph

Der Hackerparagraph, offiziell § 202c des Strafgesetzbuchs (StGB), ist eine deutsche Rechtsvorschrift, die sich mit der Vorbereitung des Ausspähens und Abfangens von Daten befasst. Diese Regelung wurde 2007 eingeführt, um Computerkriminalität zu bekämpfen. Der Paragraph stellt folgende Handlungen unter Strafe:

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Probleme des Hackerparagraphen:

- Rechtliche Grauzone: IT-Sicherheitsexperten bewegen sich oft in einer rechtlichen Grauzone, wenn sie Software auf Schwachstellen testen:

Soll etwa die Sicherheit von Zugängen getestet werden, testen Sicherheitsexperten oft, ob häufig genutzte Passwörter “Pizza123“, “adminadmin“, ...) genutzt wurden. Dafür müssen Sicherheitsexperten entsprechende Passwortlisten sammeln und vorhalten. Dies ist technisch gesehen nicht legal.

- Behinderung der Sicherheitsforschung: Hacker und Sicherheitsforscher, die für unsere digitale Sicherheit sorgen, indem sie gezielt nach Schwachstellen suchen und diese melden, gehen oft selbst rechtliche Risiken ein. Ihre Arbeit ist oft kaum möglich, ohne sich selbst strafbar zu machen. Dies kann dazu führen, dass wichtige Sicherheitslücken aus Angst vor Strafverfolgung nicht gemeldet werden, was der Sicherheit aller schadet.

- Kontraproduktive Wirkung: Statt Cyberkriminalität zu bekämpfen, kann der Paragraph dazu führen, dass legitime Sicherheitsforschung behindert wird. Dies könnte letztendlich die IT-Sicherheit insgesamt schwächen.
- Unklare Abgrenzung: Es ist oft schwierig zu unterscheiden, ob ein Tool oder eine Handlung für legitime Sicherheitszwecke oder für kriminelle Aktivitäten gedacht ist.
- Kontroverse Urteile: Ein aktueller Fall, bei dem ein IT-Spezialist wegen der Aufdeckung einer Sicherheitslücke angeklagt wurde, hat die Problematik des Paragraphen deutlich gemacht. [1]

Abschließend lässt sich sagen: Während der so genannte Hackerparagraph zum Bekämpfen von Computerkriminalität gedacht war, bewirkt er heute eher das Gegenteil:

Sicherheitsforscher und solche die es werden wollen, werden in ihrer alltäglichen Arbeit behindert, da nicht nur ihr Handwerkszeug kriminalisiert wird, sondern sie zudem beim Melden von gefundenen Sicherheitslücken Gefahr laufen, sich selbst in rechtliche Schwierigkeiten zu bringen.

Insbesondere dieses Melden gefundener Sicherheitslücken ist in unseren Augen ein nicht zu unterschätzender Beitrag zur IT-Sicherheit und kommt der Öffentlichkeit zugute. Dies unter Strafe zu stellen, schadet der Allgemeinheit und steht im starken Kontrast zu den ursprünglichen Intentionen des Gesetzes: Gut gedacht, schlecht umgesetzt!

Wir fordern, dass der sogenannte Hackerparagraph überarbeitet wird, um legitime Sicherheitsforschung zu schützen und klare Regelungen für verantwortungsvolle Offenlegung (Responsible Disclosure) von Sicherheitslücken festzulegen, die Strafverfolgung verhindern.
Quelle

[1] `https://www.justiz.nrw.de/nrwe/lgs/aachen/lg_aachen/j2023/60_Qs_16_23_Urteil_20230727.html`

PdF– Partei des Fortschritts

Verwaltungssitz
Esserstr. 2
51105 Köln