

Antrag 136/I/2023**Forum Netzpolitik****Der Landesparteitag möge beschließen:****Der Bundesparteitag möge beschließen:****Rechtssicherheit für IT-Sicherheitsforschung schaffen**

1 Wir benötigen Rechtssicherheit für IT-
2 Sicherheitsforscher*innen beim sog. Hackerparagraph §
3 202c StGB. Die Bundesregierung sollte sich dem unver-
4 züglich annehmen. Diejenigen, die ethisches Hacking
5 für IT-Sicherheit in unser aller Interesse und oft in ihrer
6 Freizeit betreiben, müssen klar und rechtssicher von den
7 Straftatbeständen ausgenommen werden.

8
9 Die gängigen Regeln zu ethischem Hacken sind von
10 den Hacker*innen einzuhalten. Insbesondere "Respon-
11 sible Disclosure", also die Nicht-Veröffentlichung der Sicher-
12 heitslücken in einem abgestimmten Zeitraum, ist Voraus-
13 setzung für ethisches Hacken.

14
15 Jede Behörde sollte Prozesse für die Beteiligung eines sol-
16 chen Verfahrens etablieren und eine Kontaktstelle für Si-
17 cherheitsforschende einrichten. Es sollte zudem juristisch
18 geprüft werden, ob ethisches Hacken ohne expliziten Auf-
19 trag von den Bundesbehörden für IT-Sicherheit für ihre Tä-
20 tigkeiten monetär kompensiert werden kann.

21
22 **Begründung**
23 Ethisches Hacken wird typischerweise von Unternehmen
24 genutzt, um ihre Systeme auf Sicherheitslücken zu prüfen.
25 Anstatt von böartigen Hackern gehackt zu werden, be-
26 zahlen sie gutwillige, um sich vor wahrhaft schädlichen
27 Attacken zu schützen. Oft werden Hacker für den Fund
28 von Sicherheitslücken bezahlt, für die sie nicht aktiv von
29 Unternehmen beauftragt wurden. Wichtig ist dabei, dass
30 die Sicherheitslücken nicht an die Öffentlichkeit getragen
31 werden ("Full Disclosure"). Zwischen den beteiligten Par-
32 teien wird die Lücke in einem abgestimmten Zeitraum erst
33 gemeldet und dann bearbeitet ("Responsible Disclosure").
34 Das hilft dabei, den Schaden für das Unternehmen zu min-
35 dern.

36
37 Im öffentlichen Sektor ist diese Praxis nicht gängig. Zwar
38 finden regelmäßig beauftragte Hacks (sog. Penetrations-
39 oder PenTests) beim BSI selbst oder durch Unternehmen
40 statt. Unabhängige Sicherheitsforschende werden aber
41 oft von der Verwaltung als Angreifer gesehen. Da ihre Tä-
42 tigkeit oft im Ehrenamt oder in ihrer Freizeit passiert, wer-
43 den sie vom Melden von Sicherheitslücken abgeschreckt.
44 Das Problem: Viele Sicherheitslücken bleiben so für die
45 Verwaltung unentdeckt und ein Einfallstor für böartige
46 Hacker.

47

Empfehlung der Antragskommission**Annahme (Konsens)**

48 Der Hackerparagraph bietet in der aktuellen Fassung kei-
49 ne Rechtssicherheit für ethisches Hacking. Sicherheitsfor-
50 schende sehen sich immer wieder strafrechtlichen Ver-
51 fahren ausgesetzt, wenn Unternehmen oder Organisatio-
52 nen Strafanzeige wegen des Ausspähens von Daten stel-
53 len. Denn es ist für Sicherheitsforschende nicht rechts-
54 sicher abschätzbar, wann der Paragraph überhaupt an-
55 wendbar ist. Die Norm regelt eigentlich eine Vorberei-
56 tungshandlung für Computerstraftaten, nach der zum
57 Beispiel Erwerb oder Herstellung von Programmen, de-
58 ren Zweck das Ausspähen von Daten ist, strafbar ist. Für
59 Sicherheitsforschende, aber auch für IT-Dienstleister be-
60 steht dadurch ein großer Graubereich, da viele Program-
61 me, die unter diese Definition fallen, auch für legale Nut-
62 zungen geeignet und nötig sind. Der Tatbestand sieht je-
63 doch keine Ausnahmen vor.

64

65 Auch wenn in der Regel die Fälle nicht zu Verurteilungen
66 führen, weil die Strafverfolgungsbehörden die Verfahren
67 mit der Begründung einstellen, dass die Tat zwar tatbe-
68 standlich gegeben, aber vermutlich nicht rechtswidrig sei,
69 ist der Verteidigungsaufwand für die meist ehrenamtlich
70 tätigen nicht nur finanziell eine ernste Belastung. Es soll-
71 te deshalb klargestellt werden, dass diejenigen, die die-
72 se wichtige Arbeit für die IT-Sicherheit in unser allem In-
73 teresse und zum Wohle der Allgemeinheit leisten, nicht
74 durch das Strafrecht bedroht werden und klar und rechts-
75 sicher von der Anwendung des "Hackerparagraphen" aus-
76 genommen sind.