

18. Rechtssicherheit für IT-Sicherheitsforschung schaffen

Die Kreisdelegiertenversammlung wolle beschließen:

Der Landesparteitag möge beschließen:

Der Bundesparteitag möge beschließen:

1 Wir benötigen Rechtssicherheit für IT-Sicherheitsforschende beim sog. Hacker-
2 paragraph § 202c StGB. Die Bundesregierung sollte sich dem unverzüglich an-
3 nehmen. Diejenigen, die ethisches Hacking für IT-Sicherheit in unser aller Inte-
4 resse und oft in ihrer Freizeit betreiben, müssen klar und rechtssicher von den
5 Straftatbeständen ausgenommen werden.

6 Die gängigen Regeln zu ethischem Hacken sind von den Hacker*innen einzu-
7 halten. Insbesondere „Responsible Disclosure“, also die Nicht-Veröffentlichung
8 der Sicherheitslücken in einem abgestimmten Zeitraum, ist Voraussetzung für
9 ethisches Hacken.

10 Jede Behörde sollte Prozesse für die Beteiligung eines solchen Verfahrens etab-
11 lieren und eine Kontaktstelle für Sicherheitsforschende einrichten. Es sollte zu-
12 dem juristisch geprüft werden, ob und wie Sicherheitsforschende ohne explizi-
13 ten Auftrag von den Bundesbehörden für IT-Sicherheit für ihre Tätigkeiten mo-
14 netär kompensiert werden kann.

15

16 **Begründung:**

17 Ethisches Hacken wird typischerweise von Unternehmen genutzt, um ihre Sys-
18 teme auf Sicherheitslücken zu prüfen. Anstatt von böartigen Hackern gehackt
19 zu werden, bezahlen sie gutwillige, um sich vor wahrhaft schädlichen Attacken
20 zu schützen. Oft werden Hacker für den Fund von Sicherheitslücken bezahlt,
21 für die sie nicht aktiv von Unternehmen beauftragt wurden. Wichtig ist dabei,
22 dass die Sicherheitslücken nicht an die Öffentlichkeit getragen werden („Full
23 Disclosure“). Zwischen den beteiligten Parteien wird die Lücke in einem abge-
24 stimmten Zeitraum erst gemeldet und dann bearbeitet („Responsible Disclo-
25 sure“). Das hilft dabei, den Schaden für das Unternehmen zu mindern.

26

27 Im öffentlichen Sektor ist diese Praxis nicht gängig. Zwar finden regelmäßig
28 beauftragte Hacks (sog. Penetrations- oder PenTests) beim BSI selbst oder
29 durch Unternehmen statt. Unabhängige Sicherheitsforschende werden aber oft
30 von der Verwaltung als Angreifer*innen gesehen. Da ihre Tätigkeit oft im Eh-
31 renamt oder in ihrer Freizeit passiert, werden sie vom Melden von Sicherheits-
32 lücken abgeschreckt. Das Problem: Viele Sicherheitslücken bleiben so für die
33 Verwaltung unentdeckt und ein Einfallstor für böartige Hacker.

34

35 Der Hackerparagraph bietet in der aktuellen Fassung keine Rechtssicherheit für
36 ethisches Hacking. Sicherheitsforschende sehen sich immer wieder strafrechtli-
37 chen Verfahren ausgesetzt, wenn Unternehmen oder Organisationen

1 Strafanzeige wegen des Ausspähens von Daten stellen. Denn es ist für Sicher-
2 heitsforschende nicht rechtssicher abschätzbar, wann der Paragraph überhaupt
3 anwendbar ist. Die Norm regelt eigentlich eine Vorbereitungshandlung für
4 Computerstraftaten, nach der zum Beispiel Erwerb oder Herstellung von Pro-
5 grammen, deren Zweck das Ausspähen von Daten ist, strafbar ist. Für Sicher-
6 heitsforschende, aber auch für IT-Dienstleister besteht dadurch ein großer
7 Graubereich, da viele Programme, die unter diese Definition fallen, auch für le-
8 gale Nutzungen geeignet und nötig sind. Der Tatbestand sieht jedoch keine
9 Ausnahmen vor.

10
11 Auch wenn in der Regel die Fälle nicht zu Verurteilungen führen, weil die Straf-
12 verfolgungsbehörden die Verfahren mit der Begründung einstellen, dass die Tat
13 zwar tatbestandlich gegeben, aber vermutlich nicht rechtswidrig sei, ist der
14 Verteidigungsaufwand für die meist ehrenamtlich tätigen nicht nur finanziell
15 eine ernste Belastung. Es sollte deshalb klargestellt werden, dass diejenigen,
16 die diese wichtige Arbeit für die IT-Sicherheit in unser allem Interesse und zum
17 Wohle der Allgemeinheit leisten, nicht durch das Strafrecht bedroht werden
18 und klar und rechtssicher von der Anwendung des „Hackerparagraphen“ aus-
19 genommen sind.

<i>Abstimmung KDV</i>	
Zustimmung	