

# Dringlichkeitsantrag

**Initiator\*innen:** Ben Lüdke (KV Steinburg) + Mark Hermandung (KV Plön)

**Titel:** **Die Hacker-Paragraphen (§202a ff. StGB)  
gerechter gestalten, unsere Gesellschaft  
schützen.**

## Antragstext

1 Nicht zuletzt seit dem völkerrechtswidrigen Überfall auf die  
2 Ukraine nehmen Cyber-Attacken auf alle Bereiche der Gesellschaft  
3 zu. Uns vor diesen zu schützen, sollte unser tiefstes  
4 Eigeninteresse sein. Doch anstatt diejenigen, die in guter Absicht  
5 Zivilcourage betreiben, indem sie Sicherheitslücken suchen, finden  
6 und diese melden, zu schützen, verfolgen wir sie strafrechtlich  
7 genau so wie diejenigen, die in digitale Systeme eindringen, um  
8 Schaden anzurichten und/oder Daten zu stehlen. Dies muss sich  
9 ändern! Diejenigen, die in Zeiten hybrider Kriegsführung zur  
10 Souveränität der deutschen Gesellschaft und Wirtschaft beitragen,  
11 sollen die Rechtssicherheit haben, dass ihr couragierte Handeln  
12 nicht zu strafrechtlichen Verfolgungen führt. Die juristische  
13 Umsetzung ist dringend geboten, bereits seit einigen Jahren weist  
14 die rechtswissenschaftliche Lehre und Rechtssprechung auf den  
15 Reformbedarf hin. Kernfrage ist hierbei, ob es die korrekte  
16 Ansicht des Rechts ist, wenn  
17 Sicherheitsanalystinnen Schuld auf sich laden, selbst wenn ihre  
18 Handlungen ausschließlich der Schließung von Sicherheitslücken  
19 dienen und dafür erforderlich sind. Auch differenziert die  
20 aktuelle rechtliche Normierung nicht zwischen schweren Straftätern  
21 und solchen, die weniger Schuld auf sich geladen haben, wobei die  
22 Obergrenze des Strafmaßes als zu gering bemängelt wird. Im Jahr  
23 2024 lag diesbezüglich bereits ein entsprechender  
24 Referentenentwurf im Bundesministerium für Justiz und  
25

26 Verbraucherschutz (BMJV) vor. Leider konnte die Gesetzesnovelle  
27 nicht vor dem Ende der Ampel-Regierung in den Gesetzgebungsprozess  
28 eingebracht werden. Ebenfalls muss bei Betrachtung des  
29 Referentenentwurfes bemängelt werden, dass dieser lediglich für  
30 IT-Sicherheitsexpert\*Innen eine Tatbestandsbefreiung sowie  
31 Qualifikation für schwere Straftaten vorsieht, bestehende  
32 Rechtslücken allerdings nicht schließt, beispielsweise die  
33 fehlende Versuchsstrafbarkeit sowie die fehlende Bestrafung von  
34 Eindringen in Systeme unter Verwendung gestohler Passwörter.  
35 Zur besseren Verdeutlichung der wesentlichen Merkmale unserer  
36 Reformvorschläge ist der folgende Gesetzestext enthalten, von dem  
37 im konkreten Fall eines Dissens bei der Umsetzung dieses  
38 Beschlusses inhaltlich und sprachlich abgewichen werden darf,  
39 sofern die Wesenszüge des Antrages unberührt bleiben:  
40 Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.  
41 November 1998

42 (BGBl. I S. 3322), das zuletzt durch Artikel 2 des Gesetzes vom  
43 30. Juli 2024

44 (BGBl. 2024 I Nr. 255) geändert worden ist, wird wie folgt  
45 geändert:

46 Um Platz für den neuen Absatz (2) zu schaffen, wird der vorhandene  
47 Absatz (2) zum neuen Absatz (3). Um die Strafbarkeitslücke  
48 zwischen vorbereitender Handlung und vorsätzlicher Begehungstat zu  
49 füllen, wird in Absatz (4) der Versuch ebenfalls strafrechtlich  
50 verfolgt.

Es wird hinzugefügt: „(4) Der Versuch ist strafbar.“

51 Änderung Nr.1:

52 Der § 202a wird in Absatz 1 folgendermaßen ergänzt:  
53 "Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht  
54 für ihn bestimmt und die gegen unberechtigten Zugang besonders  
55 gesichert sind, unter Überwindung der Zugangssicherung verschafft,  
56 wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe  
57 bestraft.

58 (2) Ebenso wird bestraft, wer unbefugt sich oder einem anderen  
59 unter Anwendung von technischen Mitteln nicht für ihn bestimmte  
60 Daten aus einem nichtöffentlichen Informationssystem verschafft,  
61 einem Dritten zugänglich macht oder der Öffentlichkeit  
62 zugänglich macht.“

63 Dem § 202a werden die folgenden Absätze 5 und 6 angefügt:

64 „(5) Die Handlung ist nicht unbefugt im Sinne des Absatzes 1, wenn  
65 1. sie in der Absicht erfolgt, eine Schwachstelle oder ein anderes  
66 Sicherheitsrisiko eines informationstechnischen Systems  
67 (Sicherheitslücke) festzustellen und die für das

68 informationstechnische System Verantwortlichen, den betreibenden  
69 Dienstleister des jeweiligen Systems, den Hersteller der  
70 betroffenen IT-Anwendung oder das Bundesamt für Sicherheit in der  
71 Informationstechnik über die festgestellte Sicherheitslücke zu  
72 unterrichten und

73 2. sie zur Feststellung der Sicherheitslücke erforderlich ist.

74 (6) In besonders schweren Fällen des Absatzes 1 ist die Strafe  
75 Freiheitsstrafe von drei Monaten bis zu fünf Jahren. Ein besonders  
76 schwerer Fall liegt in der Regel vor, wenn der Täter  
77 1. einen Vermögensverlust großen Ausmaßes herbeiführt,  
78 2. aus Gewinnsucht oder gewerbsmäßig handelt oder als Mitglied  
79 einer Bande, die sich zur fortgesetzten Begehung von solchen Taten  
80 verbunden hat oder 3. durch die Tat die Verfügbarkeit,  
81 Funktionsfähigkeit,

82 Integrität, Authentizität oder Vertraulichkeit einer kritischen  
83 Infrastruktur oder die Sicherheit der Bundesrepublik Deutschland  
84 oder eines ihrer Länder beeinträchtigt.“

85 Änderung Nr. 2:

86 § 202b wird wie folgt geändert:

87 a) Der Wortlaut wird Absatz 1.

88 b) Folgender Absatz 2 wird angefügt: „§ 202a Absatz 5 und 6 gilt  
89 entsprechend.“

90 c) Absatz 3 wird geschaffen: „(3) Der Versuch ist strafbar.“

91 Änderung Nr.3

92 Der § 303a wird abgeändert gefasst:

93 „(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe  
94 wird bestraft, wer

95 1. unbefugt Daten löscht, unterdrückt, unbrauchbar macht,  
96 verändert, oder  
97 2. unbefugt einen Programmcode in ein Informationssystem  
98 einschleust.

99 (2) Der Versuch ist strafbar.

100 (3) Für die Vorbereitung einer Straftat nach Abs.1 gilt § 202c  
101 entsprechend.“

102 Eine Verfolgungsabsicht dieser Novelle kann bei der aktuellen  
103 Bundesregierungskoalition nicht erkannt werden. Sie verzichtet  
104 somit auf die Möglichkeit, Deutschland im digitalen Raum ohne  
105 zusätzliche finanzielle Belastung sicherer zu gestalten. Ein  
106 solches Handeln ist grob fahrlässig und in der aktuellen Zeit  
107 hybrider Kriegsführung Russlands gegen Deutschland und seine  
108 Partner ein inakzeptables Sicherheitsrisiko.

109 Daher möge der Landesparteitag von BÜNDNIS 90/DIE GRÜNEN  
110 Schleswig-Holstein folgendes beschließen: BÜNDNIS 90/DIE GRÜNEN  
111 Schleswig-Holstein wird sich, sofern die Bundesregierung weiterhin

113 ein Handeln unterlässt, im Rahmen der Beteiligung an  
114 der Landesregierung in Schleswig-Holstein für eine  
115 Gesetzesinitiative im Bundesrat einsetzen, die den genannten  
116 Referentenentwurf in der o.g. abgewandelten Version weiter  
verfolgt.