

Antrag 153/I/2022**Forum Netzpolitik****Der Landesparteitag möge beschließen:****Empfehlung der Antragskommission****Annahme (Konsens)****Cyber-Resilienz Berlins stärken**

1 den Berliner Senat aufzufordern, seine präventiven Maß-
2 nahmen zum Schutz der kritischen Infrastrukturen Berlins
3 zu verbessern. Schnellstmöglich muss eine Kontaktstelle
4 bei der Senatsverwaltung für Inneres, Digitalisierung und
5 Sport (SenInnDS) i. S. d. IT-SiG eingerichtet werden. Zu-
6 dem braucht es eine klare Zuständigkeit im Berliner Senat
7 zur regelmäßigen Erarbeitung einer Cyber-Risikoanalyse
8 sowie eines risikoübergreifenden „Country-Continuity-
9 Managements“. Zur Erarbeitung der Risikoanalysen und
10 Country-Continuity-Managementpläne muss ein Netz-
11 werk zwischen den Berliner KRITIS-Betreibern, den Sicher-
12 heitsbehörden und dem Senat etabliert und gepflegt wer-
13 den. Zudem sollte der Senat proaktiv in die Kooperation
14 mit den Berliner KMUs gehen, ihnen Informationen und
15 Übungen anbieten. Berlin braucht zudem eine:n Chief
16 Information Security Officer (CISO), der mit ausreichend
17 Personal ausgestattet wird, und regelmäßige Szenarien-
18 Übungen für Katastrophenfälle.

19

20

Begründung

22 Kritische Infrastrukturen (KRITIS) sind nicht nur in aktuel-
23 len Zeiten – Zeiten in denen wieder Krieg in Europa einge-
24 zogen ist – besonders schützenswert.

25 Der Katastrophen- und Bevölkerungsschutz ist in
26 Deutschland föderal organisiert. Länder sind für die
27 Gefahrenabwehr zuständig. Dies umfasst auch die
28 Warnung der Bürger:innen im Katastrophenfall. Davon
29 ausgenommen sind militärische Angriffe, denn dieser
30 Bereich liegt im Zuständigkeitsfeld des Bundes. Auf-
31 grund dessen, dass die Ursache eines Cyberangriffs oft
32 nicht direkt ersichtlich ist, sind die Länder der zentrale
33 Verantwortungsträger.

34 Angenommen es gäbe einen Ransomware-Angriff auf die
35 Berliner Wasserwerke, der die Wasserversorgung Berlins
36 lahmlegen würde. Hier wäre die Senatsverwaltung für In-
37 neres, Digitalisierung und Sport (SenInnDS) in der Verant-
38 wortung geeignete Maßnahmen zu ergreifen die Versor-
39 gungssicherheit sowie Sicherheit und Ordnung der Bevöl-
40 kerung sicherzustellen.

41 Insbesondere im Cybersicherheitsbereich ist der Senat je-
42 doch ungenügend involviert.

43

44 Grund dabei sind folgende Problemfelder:

- 45 1. Obwohl schon mit dem ersten IT-Sicherheitsgesetz
46 aus dem Jahr 2015 feststand, dass eine Kontaktstelle
47 auf Senatsebene einzurichten sei, erfolgte dies bis
48 heute noch nicht;

- 49 2. Es gibt keine Stelle im Senat, die kontinuierlich über-
50 prüft wo die Abhängigkeiten zwischen den kriti-
51 schen Infrastrukturen vorherrschen (d.h. welche an-
52 dere KRITIS betroffen wäre);
- 53 3. Der Senat hat zudem mangelnde Kenntnisse über
54 die Abhängigkeiten der KRITIS-Betreiber von pro-
55 prietären IT-Lösungen anderer Staaten (Risiko:
56 durch die Cloudifizierung aller Bereiche erhöhen
57 sich allerdings Abhängigkeiten und in Konflikten
58 kann dies instrumentalisiert werden);
- 59 4. Anders als in Unternehmen (Unternehmen haben
60 einen Business-Continuity-Plan für den Notfall), ha-
61 ben Länder kein organisiertes und zentral gesteu-
62 ertes „Country-Continuity-Management“ für Cyber-
63 Krisen;
- 64 5. Anders als innerhalb der KRITIS Unternehmen gibt
65 es in Ländern keine regelmäßigen, organisierten
66 und strukturierten Cyber-Risikoanalysen zur prä-
67 ventiven Stärkung der Cyber-Resilienzen;
- 68 6. In Berlin sind 98% der Unternehmen
69 KMUs: sie haben meist keine bis kaum IT-
70 Sicherheitsschutzmaßnahmen und sind auf
71 staatliche Unterstützung angewiesen;
- 72 7. Die KRITIS-Betreiber sind auf Bundesebene teilwei-
73 se organisiert, aber nicht innerhalb des Land Berlin –
74 es gibt keine einheitliche Landesdefinition und kein
75 organisiertes Netzwerk;
- 76 8. Berlin hat keine:n Chief Information Security Officer
77 (CISO), d.h. Cybersicherheit wird noch nicht als stra-
78 tegische Aufgabe des Landes verstanden und bear-
79 beitet. Dies kann dazu führen, dass das Thema in Di-
80 gitalisierungsprojekten nicht genügend Beachtung
81 findet oder andere strukturelle Schwachstellen ent-
82 stehen.
- 83