Antrag 153/I/2022
Forum Netzpolitik
Der Landesparteitag möge beschließen:

Empfehlung der Antragskommission
Annahme (Konsens)

Cyber-Resilienz Berlins stärken

den Berliner Senat aufzufordern, seine präventiven Maßnahmen zum Schutz der kritischen Infrastrukturen Berlins zu verbessern. Schnellstmöglich muss eine Kontaktstelle bei der Senatsverwaltung für Inneres, Digitalisierung und Sport (SenInnDS) i. S. d. IT-SiG eingerichtet werden. Zudem braucht es eine klare Zuständigkeit im Berliner Senat zur regelmäßigen Erarbeitung einer Cyber-Risikoanalyse sowie eines risikoübergreifenden „Country-Continuity-Managements". Zur Erarbeitung der Risikoanalysen und Country-Continuity-Managementpläne muss ein Netzwerk zwischen den Berliner KRITIS-Betreibern, den Sicherheitsbehörden und dem Senat etabliert und gepflegt werden. Zudem sollte der Senat proaktiv in die Kooperation mit den Berliner KMUs gehen, ihnen Informationen und Übungen anbieten. Berlin braucht zudem eine:n Chief Information Security Officer (CISO), der mit ausreichend Personal ausgestattet wird, und regelmäßige Szenarien-Übungen für Katastrophenfälle.

Begründung
Kritische Infrastrukturen (KRITIS) sind nicht nur in aktuellen Zeiten – Zeiten in denen wieder Krieg in Europa eingezogen ist – besonders schützenswert.
Der Katastrophen- und Bevölkerungsschutz ist in Deutschland föderal organisiert. Länder sind für die Gefahrenabwehr zuständig. Dies umfasst auch die Warnung der Bürger:innen im Katastrophenfall. Davon ausgenommen sind militärische Angriffe, denn dieser Bereich liegt im Zuständigkeitsfeld des Bundes. Aufgrund dessen, dass die Ursache eines Cyberangriffs oft nicht direkt ersichtlich ist, sind die Länder der zentrale Verantwortungsträger.
Angenommen es gäbe einen Ransomware-Angriff auf die Berliner Wasserwerke, der die Wasserversorgung Berlins lahmlegen würde. Hier wäre die Senatsverwaltung für Inneres, Digitalisierung und Sport (SenInnDS) in der Verantwortung geeignete Maßnahmen zu ergreifen die Versorgungssicherheit sowie Sicherheit und Ordnung der Bevölkerung sicherzustellen.
Insbesondere im Cybersicherheitsbereich ist der Senat jedoch ungenügend involviert.

Grund dabei sind folgende Problemfelder:

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

2. Es gibt keine Stelle im Senat, die kontinuierlich überprüft wo die Abhängigkeiten zwischen den kritischen Infrastrukturen vorherrschen (d.h. welche andere KRITIS betroffen wäre);
3. Der Senat hat zudem mangelnde Kenntnisse über die Abhängigkeiten der KRITIS-Betreiber von proprietären IT-Lösungen anderer Staaten (Risiko: durch die Cloudifizierung aller Bereiche erhöhen sich allerdings Abhängigkeiten und in Konflikten kann dies instrumentalisiert werden);
4. Anders als in Unternehmen (Unternehmen haben einen Business-Continuity-Plan für den Notfall), haben Länder kein organisiertes und zentral gesteuertes „Country-Continuity-Management“ für Cyber-Krisen;
5. Anders als innerhalb der KRITIS Unternehmen gibt es in Ländern keine regelmäßigen, organisierten und strukturierten Cyber-Risikoanalysen zur präventiven Stärkung der Cyber-Resilienzen;
6. In Berlin sind 98% der Unternehmen KMUs: sie haben meist keine bis kaum IT-Sicherheitsschutzmaßnahmen und sind auf staatliche Unterstützung angewiesen;
7. Die KRITIS-Betreiber sind auf Bundesebene teilweise organisiert, aber nicht innerhalb des Land Berlin – es gibt keine einheitliche Landesdefinition und kein organisiertes Netzwerk;
8. Berlin hat keine:n Chief Information Security Officer (CISO), d.h. Cybersicherheit wird noch nicht als strategische Aufgabe des Landes verstanden und bearbeitet. Dies kann dazu führen, dass das Thema in Digitalisierungsprojekten nicht genügend Beachtung findet oder andere strukturelle Schwachstellen entstehen.