Interpellation Nr. 6 (Februar 2023)
betreffend den Schutz kritischer Infrastrukturen vor Cyber-Risiken

23.5037.01

Die in der Schweiz rasch voranschreitende Digitalisierung bedeutet für Wirtschaft und Gesellschaft grosse Effizienzgewinne. Prozesse werden vereinfacht und die Kommunikation revolutioniert. Neben diesen Chancen entstehen auch Risiken. Wirtschaft und Gesellschaft werden zunehmend abhängig von Informations- und Kommunikationstechnologien, wodurch auch deren Verwundbarkeit steigt. Die stark zunehmenden Bedrohungen im Cyberraum sind vielfältig. Neben der Cyber-Kriminalität, der Cyber-Spionage und der Verwendung von mittels Cyber-Angriffen entwendeten oder manipulierten Informationen für Propagandazwecke stellt insbesondere die Cyber-Sabotage bei kritischen Infrastrukturen die Gesellschaft und die Unternehmen vor grosse Herausforderungen.

Diese Risiken haben sich mit dem Ausbruch des Krieges in der Ukraine und der Konfrontation zwischen Russland und dem Westen – etwa als Reaktion auf die westlichen Sanktionen – auch für die Schweiz verschärft. Rund 34'400 Meldungen zu Cyberangriffen hat das Nationale Zentrum für Cybersicherheit im Jahr 2022 erhalten. Dies sind fast 60 Prozent mehr als im Vorjahr.

Es ist für das Funktionieren des Wirtschaftsstandortes Basel und für die einzelnen Unternehmen essenziell, dass die kritische Infrastruktur – nicht zuletzt im Energiebereich – vor unberechtigtem Zugriff geschützt wird und die Versorgungssicherheit gewährleistet bleibt. Dieser Vorstoss zielt deshalb nicht auf die in anderen Vorstössen angesprochene klassische Cyber-Kriminalität, sondern explizit auf den Schutz der kritischen Infrastruktur vor Cyber-Risiken.

Welche Elemente konkret als kritische Infrastrukturen gelten, wird im als «geheim» klassifizierten Inventar der kritischen Infrastruktur-Elemente des Bundesamtes für Bevölkerungsschutz definiert. Darin enthalten sind wichtige Bauten und Anlagen aus neun Sektoren, darunter Gesundheit, Finanzen, Verkehr und Energie. Die kritische Infrastruktur im Bereich Energie umfasst beispielsweise alle Einrichtungen und Tätigkeiten, die für die Belieferung der Verbraucher mit Energie erforderlich sind (Kraftwerke, Energienetze, Infrastrukturen für die Systemkoordination und Netzregelung, Transportinfrastrukturen etc.).

Der Bundesrat hat bereits vor Ausbruch des Ukrainekrieges erkannt, dass die Schweiz ihre Resilienz gegenüber Cyber-Vorfällen erhöhen muss. Er hat deshalb mit der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018 – 2022 (NCS)» in Zusammenarbeit mit den Kantonen und der Wirtschaft ein Papier vorgelegt, welches die Schutzmassnahmen der unterschiedlichen Akteure koordiniert. Im dazugehörenden Umsetzungsplan der Kantone, den die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) im Frühling 2019 genehmigte, wird die kantonale Umsetzung der in der NCS definierten Handlungsfelder festgelegt. Dazu gehören unter anderem Massnahmen wie die Entwicklung eines kantonalen Cyberbedrohungsradars, die Einführung einer kantonseigenen Netzwerk-Sicherheits-Policy und eines kantonalen Cyberkonzepts, die Durchführung einer Cyberübung mit kritischen Infrastrukturen im Gesundheitssektor sowie die Schaffung einer kantonalen Organisation für Cyber-Sicherheit. Diesen kommt aufgrund der angespannten geopolitischen Lage zusätzliche Dringlichkeit zu.

Im Jahresbericht des Sicherheitsverbundes Schweiz wird Auskunft über die «erreichten Meilensteine» erteilt. Diese sind jedoch nicht auf die einzelnen Kantone aufgeschlüsselt. Wir bitten den Regierungsrat deshalb, über den aktuellen Umsetzungsstand des Kantons Basel-Stadt bezüglich der im Umsetzungsplan der Kantone definierten Massnahmen sowie weitere Aktivitäten zum Schutz der kritischen Infrastruktur Auskunft zu erteilen. Ein ähnlich lautender Vorstoss wird auch im Kanton Basel-Landschaft eingereicht.

Wir bitten den Regierungsrat deshalb, die folgenden Fragen zu beantworten:

1. Wie schätzt der Regierungsrat die aktuelle Bedrohungslage für die kritischen Infrastrukturen des Kantons Basel-Stadt (insbesondere im Energiesektor) durch Cyber-Gefahren ein?
2. Welche Massnahmen aus dem Umsetzungsplan der Kantone wurden im Kanton Basel-Stadt bereits umgesetzt bzw. was ist deren Umsetzungsstand?
3. Wie sieht der aktuelle Zeitplan des Kantons Basel-Stadt zur Umsetzung der Massnahmen aus dem Umsetzungsplan der Kantone aus?

4. Schätzt der Regierungsrat die im Umsetzungsplan der Kantone aufgeführten Massnahmen als genügend für den Schutz der kritischen Infrastrukturen (insbesondere im Energiesektor) vor Cyber-Risiken im Kanton Basel-Stadt ein und wie kommt er zu dieser Einschätzung?
5. Welche über den Umsetzungsplan der Kantone hinausgehenden Massnahmen hat der Kanton Basel-Stadt zum Schutz von kritischen Infrastrukturen (insbesondere im Energiesektor) durch Cyber-Risiken ergriffen oder geplant?
6. Inwiefern besteht ein Austausch zwischen den kantonalen Behörden und den Betreibern von kritischen Infrastrukturen in Bezug auf die Bewältigung von Cyber-Risiken?

Beat Braun