Regierungsrat des Kantons Basel-Stadt

An den Grossen Rat **23.5037.02**

FD/P235037

Basel, 8. März 2023

Regierungsratsbeschluss vom 7. März 2023

Interpellation Nr. 6 von Beat Braun betreffend «den Schutz kritischer Infrastrukturen vor Cyber-Risiken»

(Eingereicht vor der Grossratssitzung vom 8. Februar 2023)

«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»

Wir beantworten diese Interpellation wie folgt:

1. Einleitung

1.1 Nationale Strategie zum Schutz kritischer Infrastrukturen

Die vom Bundesrat am 8. Dezember 2017 für den Zeitraum 2018 bis 2022 verabschiedete nationale Strategie zum Schutz kritischer Infrastrukturen (SKI-Strategie) definiert 17 Massnahmen, mit denen der Bundesrat die Versorgungssicherheit in der Schweiz erhalten und in wesentlichen Bereichen verbessern will.

1.2 Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken / Umsetzungsplan der Kantone zur nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken

Zur Steigerung der Resilienz vor Cyber-Angriffen verabschiedete der Bundesrat am 18. April 2018 die zusammen mit den Kantonen und der Wirtschaft erarbeitete Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS 2018 - 2022). Zu diesem nationalen Umsetzungsplan erarbeitete eine Arbeitsgruppe des Sicherheitsverbundes Schweiz (SVS) im Frühjahr 2019 den Umsetzungsplan der Kantone. Dieser präsentiert sich eigenständig, aber komplementär zum nationalen Umsetzungsplan. Konkret handelt es sich um 13 Umsetzungsprojekte in sieben von zehn Handlungsfeldern der NCS.

1.3 Kantonale Strategie für den Schutz von kritischen Infrastrukturen

Eine Arbeitsgruppe, zusammengesetzt aus verschiedenen Disziplinen, hat unter der Leitung der Kantonalen Krisenorganisation Basel-Stadt (KKO) sowie der Fachstelle Gefahrenprävention am Kantonalen Laboratorium ein Pendant zur nationalen SKI-Strategie auf kantonaler Ebene erarbeitet. Diese Kantonale SKI-Strategie hat zum Ziel, die Resilienz im Kanton im Hinblick auf kritische Infrastrukturen zu verbessern und damit zum Schutz der Bevölkerung, zur Erhaltung des wirtschaftlichen Wohlstands und zur Sicherheit des Kantons beizutragen. Sie hält fest, welche Ziele der Kanton verfolgt, und zeigt auf, welche Massnahmen getroffen werden, um die Resilienz des Kantons in Bezug auf kritische Infrastrukturen – auch gegen Cyberbedrohungen – zu verbessern.

2. Zu den einzelnen Fragen

1. Wie schätzt der Regierungsrat die aktuelle Bedrohungslage für die kritischen Infrastrukturen des Kantons Basel-Stadt (insbesondere im Energiesektor) durch Cyber-Gefahren ein?

Der Regierungsrat teilt die Meinung des Interpellanten, dass Cyber-Angriffe ein wesentliches Risiko für öffentliche Organisationen und versorgungskritische Infrastrukturen und Systeme sind und dass die Wahrscheinlichkeit für solche Angriffe zunimmt.

Wie viele grosse Betriebe der Privatwirtschaft, haben im Kanton Basel- Stadt kritische Infrastrukturen wie beispielsweise IWB konkrete Massnahmen ergriffen und umgesetzt. Diese umfassen u.a. die Erhöhung der Netzwerksicherheit, die Schaffung von Sicherheitsstandards sowie die Implementierung von Betriebskontinuitätsmanagement in der IT-Landschaft.

2. Welche Massnahmen aus dem Umsetzungsplan der Kantone wurden im Kanton Basel-Stadt bereits umgesetzt bzw. was ist deren Umsetzungsstand?

Einige der Massnahmen aus dem Umsetzungsplan wurden bereits umgesetzt, während andere sich noch in der Umsetzung befinden oder geplant sind. So wurde beispielsweise bei der Staatsanwaltschaft im Bereich der Kriminalitätsbekämpfung das Dezernat Digitale Kriminalität geschaffen, welches seit 2021 in Betrieb ist. Im Bereich Resilienzmanagement werden die Abhängigkeiten von Systemen und anderen Dienstleistenden erhoben. Ebenso sind die wichtigsten IKT-Anwendungen und Verbindungen definiert und die geforderte Verfügbarkeit ermittelt, um die Resilienz entsprechend erhöhen zu können. In der kantonalen Verwaltung wird mit dem Projekt «Sicherheits-Monitoring» insbesondere auf Früherkennung, konsequente Dokumentation und Sensibilisierung gesetzt. Punkto Sensibilisierung ist im laufenden Jahr eine Awareness-Kampagne zu Cyber-Risiken geplant. Dies mit dem Ziel, das Sicherheitsbewusstsein der kantonalen Mitarbeitenden weiter zu erhöhen.

Konkret sieht der Umsetzungsplan der Kantone sechs Handlungsfelder vor. Folgende wesentlichen Aktivitäten in Basel-Stadt seien erwähnt:

- **Handlungsfeld 1 / Kompetenzen- und Wissensaufbau**
  Der Sicherheitsverbund Schweiz (SVS) hat eine zentrale eLearning Plattform aufgebaut. Die Variante Basel-Stadt befindet sich in Finalisierung.
- **Handlungsfeld 2 / Bedrohungslage**
  Das Nationale Zentrum für Cybersicherheit (NCSC) hat eine gemeinsame Plattform für Bund und Kantone aufgebaut. Basel-Stadt hat Zugriff und partizipiert aktiv.
- **Handlungsfeld 3 / Resilienzmanagement**
  Das NCSC stellt eine strukturierte Umfrage zur Verfügung, bei welcher Basel-Stadt aktiv mitmacht und regelmässig neue Erkenntnisse erhält.
- **Handlungsfeld 4 / Standardisierung/Regulierung**
  Basel-Stadt gehört zu den wenigen Kantonen, die eine kantonseigene Netzwerksicherheitspolicy (NSP.BS) kennt und anwendet.

- **Handlungsfeld 5 / Krisenmanagement**
  Die Federführung liegt beim Bund. Basel-Stadt ist aktiv involviert.
- **Handlungsfeld 6 Aussenwirkung und Sensibilisierung**
  Aktivitäten werden regelmässig übergreifend zusammengetragen und auf der Website des SVS publiziert (svs.admin.ch).

3. Wie sieht der aktuelle Zeitplan des Kantons Basel-Stadt zur Umsetzung der Massnahmen aus dem Umsetzungsplan der Kantone aus?

Im Kanton Basel-Stadt besteht Koordinationsbedarf zur Umsetzung der Massnahmen. Der Regierungsrat hat die Verwaltung mit der entsprechenden Berichterstattung bis Sommer 2023 beauftragt. In diesem Zusammenhang soll auch die Erstellung eines Umsetzungszeitplans geprüft werden.

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

Aktuell erachtet der Regierungsrat den Umsetzungsplan als genügend. Die Bedrohungslage ist aber volatil und unvorhergesehenen Entwicklungen unterworfen.

Was die Energieversorgung angeht, kann festgestellt werden, dass die IWB bereits seit längerem einen Rahmen aufgebaut hat, mit dem der Schutz des Systems gewährleistet werden kann. Das Thema Informations- und Informatiksicherheit ist dauerhaft in Projekten und insbesondere im Infrastrukturbetrieb etabliert. Sämtliche IWB Mitarbeitende werden regelmässig geschult und auf mögliche Bedrohungen vorbereitet. Die versorgungskritischen Systeme der IWB sind redundant ausgelegt und durch Notstrom versorgt. Zudem sind die versorgungskritische ICT-Infrastruktur (OT) sowie die Steuerung und Überwachung von physischen Anlagen oder Prozessen (z.B. Heizkraftwerk) sichergestellt. Alle kritischen Systeme werden gezielt überwacht, damit Unregelmässigkeiten frühzeitig erkannt und eliminiert werden können. Darüber hinaus wird die OT-Systemlandschaft der IWB immer wieder durch Penetrationstests und Audits durch unabhängige Dritte überprüft. Wichtige Anlagen der IWB können für den Fall eines Totalausfalls der IT-Systeme auch abgekoppelt und von Hand gefahren werden.

Der Schutz und die Ausfallsicherheit der kritischen Systeme sind generell Teil des übergeordneten Betriebskontinuitätsmanagements der IWB. In diesem Rahmen werden alljährlich Notfall-Szenarien mit realbezogenen Übungen geprobt. Für alle Systeme gibt es Notfalldokumentationen und Wiederanlaufpläne. Die IT-Organisation ist integraler Bestandteil des IWB-internen Krisenstabes.

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?

Wie dargestellt hat die IWB mit Blick auf die hohe Versorgungsrelevanz im Bereich Energie schon früh und umfassend auf Risiken aus dem Datennetz reagiert. Die Stärkung der Resilienz gegenüber Cyberangriffen ist in den Geschäftsprozessen integriert. Generell forciert werden soll v.a. die Früherkennung von Cyber-Bedrohungen, wie es auch in der Informationssicherheitsstrategie Basel-Stadt von 2022 verabschiedet wurde. So können Cyber-Angriffe gegen kritische Infrastrukturen erkannt und proaktive Massnahmen lanciert werden.

6. Inwiefern besteht ein Austausch zwischen den kantonalen Behörden und den Betreibern von kritischen Infrastrukturen in Bezug auf die Bewältigung von Cyber-Risiken?

Zwischen der KKO und den Betreibenden von kritischen Infrastrukturen findet ein regelmässiger Austausch statt. Im Bereich der Energieversorgung agiert die IWB zudem in schweizweiter Vernetzung. Sie steht u.a. in einem engen Austausch mit SWITCH und NCSC, um die aktuelle Bedrohungslage zeitnah einschätzen und mit gezielten Massnahmen frühzeitig reagieren zu können.

Im Namen des Regierungsrates des Kantons Basel-Stadt

Beat Jans
Regierungspräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin