BASEL LANDSCHAFT
REGIERUNGSRAT

Vorlage an den Landrat

Beantwortung der Interpellation 2023/69 von Martin Dätwyler: «Schutz kritischer Infrastrukturen»
2023/69

vom 25. April 2023

1. Text der Interpellation

Am 26. Januar 2023 reichte Martin Dätwyler die Interpellation 2023/69 «Schutz kritischer Infrastrukturen» ein. Sie hat folgenden Wortlaut:

Die in der Schweiz 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 der regionalen Wirtschaft 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 ab, 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-Landschaft 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-Stadt eingereicht.

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

- *Wie **schätzt** der Regierungsrat die **aktuelle Bedrohungslage** für die kritischen Infrastrukturen des Kantons Basel-Landschaft (insbesondere im Energiesektor) durch Cyber-Gefahren **ein**?*
- *Welche **Massnahmen aus dem Umsetzungsplan der Kantone** wurden im Kanton Basel-Landschaft bereits umgesetzt bzw. was ist deren **Umsetzungsstand**?*
- *Wie sieht der **aktuelle Zeitplan** des Kantons Basel-Landschaft zur Umsetzung der Massnahmen aus dem Umsetzungsplan der Kantone aus?*
- *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-Landschaft ein und wie kommt er zu dieser Einschätzung?*
- *Inwiefern besteht ein **Austausch zwischen den kantonalen Behörden und den Betreibern von kritischen Infrastrukturen** in Bezug auf die Bewältigung von Cyber-Risiken?*

2. Einleitende Bemerkungen

Bund und Kantone haben die Risiken bezüglich Zunahme der Cyberkriminalität im Zusammenhang mit dem Ausbau der Digitalisierung erkannt. Im Auftrag der KKJPD erarbeiteten der Bund und die Kantone im Rahmen des Sicherheitsverbunds Schweiz (SVS) die im Interpellationstext erwähnte nationale Cyberstrategie Schweiz (NCS). Darin wird u.a. vorgesehen, dass die Kantone eine Organisation und eigene Strategien für Cybersicherheit schaffen. Eine Arbeitsgruppe des Sicherheitsverbundes Schweiz hat hierfür eine «Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation» ausgearbeitet, welche dem im Interpellationstext erwähnten Umsetzungsplan der Kantone entspricht. Der Bund hat bereits verschiedene Massnahmen umgesetzt (u.a. Aufbau Nationales Zentrum für Cybersicherheit NCSC) und auch andere Kantone haben ihre Cybersicherheit mit unterschiedlichen Massnahmen stark verbessert (Aufbau Security Operation Center SOC, Netzwerkzonierung, Malwareschutz der neuen Generation etc.). Im Kanton Basel-Landschaft sind viele dieser Massnahmen in der Planung, während parallel dazu die Digitalisierung der Verwaltung vorangetrieben wird. Ein Regierungsratsbeschluss zur Auftragserteilung für die Umsetzung der nationalen Cyberstrategie und die Erarbeitung eines Konzepts für eine zukünftige Cyberorganisation soll in den nächsten Wochen erfolgen.

3. Beantwortung der Fragen

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

Gemäss der Gefährdungsanalyse des Kantons Basel-Landschaft liegt die Eintretenswahrscheinlichkeit eines Cyber-Angriffs auf Stufe 4 von 6. Dies bedeutet, dass mit einem solchen Szenario in der normalen Lage gerechnet werden muss.

Aufgrund der aktuellen Weltlage mit den kriegerischen Ereignissen zwischen Russland und der Ukraine, hat sich das Risiko von Cyber-Angriffen auf Kritische Infrastrukturen (KI) entsprechend verschärft. Beispiele dafür ist der Sabotageakt auf das Kommunikationssystem der Deutschen Bahn vom Oktober 2022 oder jener auf die SBB im Februar 2023. Gemäss einem Bericht des IT-Beratungsunternehmens IBM zu den Hackerangriffen 2022 steht die Energie- und Gesundheitsbranche mit 10 Prozent an dritter Stelle der betroffenen Branchen (BZ Artikel 22.2.23).

Bis dato besteht für die Betreibenden von kritischen Infrastrukturen keine Meldepflicht für Cybervorfälle. Deshalb kann heute nur ein (sehr) unvollständiges Bild der aktuellen Bedrohungslage gezeichnet werden. Der Regierungsrat des Kantons Basel-Landschaft hat daher in seiner Vernehmlassungsantwort vom 29. März 2022 an das Eidg. Finanzdepartement die Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe explizit begrüsst.

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

Wie einleitend erwähnt, befindet sich der Aufbau einer kantonalen Umsetzungsorganisation im Kanton Basel-Landschaft in der Konzeptphase. Im Zuge des Aufbaus sollen weitere Massnahmen und Vorhaben realisiert werden, welche unter anderem die Ausrichtung der Informatik-Notfallvorsorge auf das Business-Continuity-Management (BCM), die Verbesserung der Versorgungssicherheit und der Resilienz gegenüber Cyberangriffen beinhalten.

Die weiteren umgesetzten oder in der Umsetzung befindlichen Massnahmen lassen sich wie folgt zusammenfassen:

M8: Entwicklung und Einführung von Minimalstandards

In der zentralen Informatik BL ist die Umsetzung der Netzwerksicherheitspolicy fortlaufend im Gang. Die Umsetzung ist etappiert über mehrere Phasen und folgt dem Ersatzinvestitionszyklus der relevanten IT-Infrastruktur-Komponenten. Aktuell ist das Projekt «Aufbau neue Network Access Control» initiiert.

Im Jahr 2023 erfolgt durch die zentrale Informatik eine Ausschreibung für den ab 2024 vorgesehenen Aufbau eines hybriden Security Operation Centers (SOC), in Zusammenarbeit mit einem externen, spezialisierten SOC-Dienstleister. Im Vordergrund steht die frühzeitige Erkennung von Informationssicherheitsrisiken, die Reaktionsfähigkeit vor Eintritt eines Sicherheitsvorfalls und die Unterstützung des Krisenmanagements bei Eintritt eines Sicherheitsereignisses (z.B. bei Datenverschlüsselung durch Ransomware). Für die Übergangszeit bis zur operativen Betriebsaufnahme eines SOC besteht ein Dienstleistungsvertrag mit einer IT-Security Dienstleisterin für technische Analyseleistungen, Szenarien-Simulation und 7x24h Unterstützung zur Bewältigung von Notfall-Ereignissen.

M18: Fallübersicht Cybercrime

Schweizweit existiert aktuell keine zentrale Plattform, bestehend aus zentraler Datenbank und Analysetool, zum Zwecke der Koordination und Analyse von seriellen Cyberstraftaten. In der West-

schweiz ist im Polizeikonkordat CLCPC die Analysesoftware PICSEL im Einsatz. In der Deutschschweiz arbeiten derzeit die Polizeikorps der Kantone Aargau und Graubünden seit dem 1. Juli 2021, respektive seit dem 1. Juli 2022, im Regelbetrieb mit PICSEL.

Im Kanton Basel-Landschaft wurde im August 2022 ein Projekt zur Einführung der Analysesoftware PICSEL gestartet. Dieses Projekt befindet sich aktuell in der Konzeptphase nach HERMES.

Auf nationaler Ebene läuft derzeit ein durch die Konferenz der kantonalen Polizeikommandantinnen und Polizeikommandanten (KKPKS) initiiertes Projekt zur schweizweiten Nutzung der Analysesoftware PICSEL, respektive der Evaluierung und Einführung einer Nachfolgelösung der bestehenden PICSEL-Lösung. Mit der Einführung einer solchen Lösung ist aber nicht vor 2025/2026 zu rechnen.

M19: Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK)

Das im Rahmen der Umsetzung der NCS geschaffene Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK) wird aus Sicht der Polizei Basel-Landschaft als grosser Mehrwert angesehen. Von besonderem Interesse sind dabei die regelmässig stattfindenden operativen Meetings und der durch NEDIK ermöglichte vereinfachte Wissenstransfer zwischen Ermittelnden.

M29: Sensibilisierung der Öffentlichkeit betreffend Cyberrisiken

Im Bereich der Prävention wurden durch die Abteilung Cybercrime der Polizei Basel-Landschaft die nachfolgend aufgeführten präventiven Anlässe für einzelne Zielgruppen und die breite Bevölkerung angeboten:

2019
- Informationsanlässe für die Bevölkerung (12.10.2019, 16.10.2019, 30.10.2019, 20.11.2019 sowie 26.11.2019)

2020
- Pandemie bedingt keine Anlässe für die Bevölkerung
- Informationsanlass für Unternehmungen (16.09.2020)

2021
- Pandemie bedingt keine Anlässe für die Bevölkerung
- An den BBZ-Standorten in Liestal und Muttenz wurden durch Mitarbeitende der Abteilung Cybercrime und dem Jugenddienst 62 Referate zu den Themen Cybercrime und Cybermobbing gehalten.

2022
- Informationsanlass für Gemeinden (18.05.2022)
- Informationsanlässe für die Bevölkerung (08.06.2022 & 07.09.2022)
- Informationsanlässe für Unternehmungen (22.06.2022 & 16.09.2022)
- An den BBZ-Standorten in Liestal und Muttenz wurden durch Mitarbeitende der Abteilung Cybercrime und dem Jugenddienst 55 Referate zu den Themen Cybercrime und Cybermobbing gehalten.

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

Wie einleitend erwähnt, erfolgt ein Konzept für eine zukünftige Cyber-Organisation bis Ende September 2023.

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-Landschaft ein und wie kommt er zu dieser Einschätzung?*

Betreffend die kritischen Infrastrukturen (KI) ist zu erwähnen, dass jede Organisation respektive jeder Betreiber einer KI für die Informationssicherheit des Betriebes verantwortlich ist. Dies ist so im Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-22 aufgeführt (Handlungsfeld 3 «Resilienzmanagement», Absatz «Beteiligung».)

Zur Unterstützung von Unternehmen ist auf der Webseite des Kompetenzzentrums Cybercrime der Link Informationen für KMU eingebunden, unter welchem verschieden Dokumente in Form von Informationsmaterial und Handlungsempfehlungen geöffnet werden können. Als weitere Quelle sei hier die Webseite des Bundesamts für wirtschaftliche Landesversorgung BWL mit den IKT-Minimalstandards und den Branchenstandards für Wasserversorgung, Abwasser, Lebensmittel, Gasversorgung, öffentlicher Verkehr, Strom, Abfallentsorgung sowie Fernwärme- um Fernkälteversorgung genannt.

Die Abteilung Cybercrime der Polizei Basel-Landschaft beteiligt sich aktiv am aktuell laufenden Aufbau der Incident Response der kantonalen Verwaltung Basel-Landschaft.

Bezüglich der Wirksamkeit der Massnahmen bei kritischen Infrastrukturen kann insbesondere auf die im Auftrag des Nationalen Zentrums für Cybersicherheit (NCSC) erstellte Wirksamkeitsüberprüfung der Nationalen Cyberstrategie 2018-2022 (Bericht «Wirksamkeitsüberprüfung 'Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018 bis 2022' vom 28. März 2022, Autoren: EPO und econcept) verwiesen werden (Ziff. 4.2). Das Fazit im Bereich kritischer Infrastrukturen lautet: «Die Betreiber/innen kritischer Infrastrukturen sind sensibilisiert und eng in die Massnahmen bzw. Umsetzungsprojekte eingebunden; es sind aber klare Unterschiede zwischen den Sektoren erkennbar. Die aus der Strategie erbrachten Leistungen reichen noch nicht aus, sämtliche kritischen Infrastrukturen angemessen zu schützen.»

Die Arbeiten beim Schutz vor Cyber-Risiken laufen also sowohl beim Bund als auch im Kanton weiter und befinden sich in einem fortlaufenden Prozess. Vor diesem Hintergrund kann der Regierungsrat kein abschliessendes Fazit über das Ausreichen der Massnahmen ziehen.

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

Der Kantonale Führungsstab trat im Zuge der Ereignisbewältigung Covid-19 mit den KI-Betreibern in direkten Kontakt und führte nebst regelmässigen Absprache-Rapporten eine Monitoring-System ein. Der Fokus lag dabei jedoch auf deren Resilienz im Hinblick auf Personalausfälle und unterbrochene Lieferketten.

Bei der Ausarbeitung von Einsatz- und Vorsorgeplanungen im Hinblick auf eine mögliche Energiemangellage wurde der Austausch mit Betreibern Kritischer Infrastrukturen wieder intensiviert. Nebst Rapporten fanden und finden themen- und branchenspezifische Stabsarbeitstage statt. Diese verfolgen das Ziel der breit abgestützten Problemerfassung und Entwicklung von Lösungsvarianten zwecks Resilienz-Stärkung. Mit dem selben Ziel unterstützt der Kantonale Führungsstab zudem die Unternehmen mit einem neuen Handbuch bei der betrieblichen Vorsorge auf eine mögliche Energiemangellage.

Im Rahmen der nationalen Strategie zum Schutz Kritischer Infrastrukturen wurden die KI von Seiten des Kantons kontaktiert und mit ihnen vorhandene Sicherheitsvorkehrungen und Dokumentationen in den Bereichen Notfallplanungen/Einsatzplanungen besprochen. Bei allen bisher kontaktierten KI sind Planungen und Konzepte im Bereich Cyber-Sicherheit vorhanden. Das Amt für Militär und Bevölkerungsschutz kann jedoch nicht den gesamten Bereich «Schutz kritischer Infrastruktur» abdecken, da dafür nur sehr begrenzte Ressourcen zur Verfügung stehen. Diesem Umstand soll mit dem erwähnten Konzept zur Schaffung einer kantonalen Cyber-Organisation begegnet werden.

Die Abteilung Cybercrime der Polizei organisiert Informationsanlässe für Unternehmungen (vgl. Frage 2), ein Institutionalisierter Austausch zwischen mit Betreibern von kritischer Infrastruktur findet bisher allerdings nicht statt.

Liestal, 25. April 2023

Im Namen des Regierungsrats

Die Präsidentin:

Kathrin Schweizer

Die Landschreiberin:

Elisabeth Heer Dietrich