



An den Grossen Rat

22.5216.03

JSD/P225216

Basel, 18. Dezember 2024

Regierungsbeschluss vom 17. Dezember 2024

Anzug Philip Karger und Konsorten betreffend Stärkung der Cybersicherheit für Staatliche Verwaltungen, Firmen und Privaten in Basel-Stadt

Der Grosse Rat hat an seiner Sitzung vom 9. November 2022 die nachstehende Motion Philip Karger und Konsorten dem Regierungsrat als Anzug überwiesen:

«Mit dem verbundenen Anstieg der Nutzung von elektronischen Geräten (Computer, Mobil-geräte und Onlineangebote) ist eine hohe Cyberkriminalität festzustellen. Fast täglich berichten die Medien von gehackten Firmen- und privaten Accounts und gestohlenen Daten oder sonstigen Verbrechen, wie Erpressung usw.

Die aktuelle Bedrohungslage ist gemäss nationalen Cybersicherheitszentrum NCSC kritisch und wird dauerhaft auch so bleiben. Die Professionalisierung von kriminellen Hackerbanden aus verschiedenen Staaten nimmt stetig zu. Oft ist den Nutzern der vielen digitalen Angeboten nicht bewusst, dass sie ihre Daten und Geräte schützen müssen und auch nicht wie. Da der Schutz von Daten Aufgabe des Staates ist, muss dieser für Aufklärung, Ahndung, Verfolgung und Sensibilisierung sorgen. Wichtig sind eine schnelle Prüfung, Anpassung und Erweiterung der Massnahmen und, da wo nötig, der Gesetzgebung. Basel-Stadt kann und soll bei der Cybersicherheit Schweizweit eine Vorreiterrolle einnehmen und die Sicherheit der verschiedenen Anspruchsgruppen erhöhen. Um diese Sicherheit zu gewährleisten, muss der Kanton, analog der Sicherheit im Verkehr, bei Kriminalität, Terrorismus und anderen Bedrohungen, die entsprechenden technischen und organisatorischen Massnahmen treffen.

Geforderte Massnahmen

Cybercrime-Meldestelle: Die Meldestelle muss so ausgebaut werden, dass alle Bürgerinnen und Bürger und alle Firmen immer und in Echtzeit, im Sinne einer Gefahrenkarte (z.B. auf map.geo.bs.ch) über Cyber-Bedrohungen aller Art informiert sind. Per Gesetz muss jede Straftat und Bedrohung sofort gemeldet werden. Auf diese Informationen muss per Alert (PUSH) und auch auf Abruf (PULL) zugegriffen werden können. Firmen, ab einer zu definierenden Grösse, müssen Cybersicherheitsbeauftragte mit Kompetenzen im Informations- und IT-Sicherheitsbereich einsetzen.

Awareness-Kampagnen: Der Kanton soll mit regelmässigen Kampagnen auf die Cyberbedrohungen aufmerksam machen und so die Bürgerinnen und Bürger sensibilisieren. Dabei sollen Prävention und Vorsichtsmassnahmen im Vordergrund stehen. Genaue Anleitungen, sowie schnelle und unkomplizierte Hilfen im Falle eines Angriffs oder Diebstahls müssen angeboten und jederzeit abrufbar sein. Das Prinzip: "Meine Daten gehören mir"; bei Firmen "Die Daten der Kunden gehören ihnen", muss bekannt und gestärkt werden. Es braucht eine Sensibilisierung im Umgang mit der Freigabe persönlicher- und Kundendaten.

Staatliche Aufgaben und Angebote: Der Kanton muss, wie bei der "physischen" Kriminalität, Prävention, Schutz und Massnahmen übernehmen. Solange der Kanton diese Aufgaben an ausserkantonale Stellen abgibt, kann er keine eigene Kompetenz aufbauen und die viele Firmen, Bürgerinnen und Bürger nehmen die Cyberkriminalität nicht ernst genug.

Personen bezogene Daten: Personenbezogene Daten sind ein sehr hohes und wertvolles Gut. Diese Daten müssen wie eine offizielle Währung behandelt und entsprechend durch technische und organisatorische Massnahmen geschützt werden. Der Kanton muss die Speicherung der sensiblen Daten, analog der monetären Verwaltung und Reserven selbst übernehmen.

Aufbau Kompetenz-Zentrum Cybercrime: Um die oben erwähnten Aufgaben bezüglich Cybercrime sicherzustellen, schlagen die Unterzeichnenden den Aufbau eines Kompetenzzentrums Cybercrime im Bereich JSD vor.

Die Unterzeichnenden bitten den Regierungsrat, die Voraussetzungen zu schaffen, damit die Cybersicherheit von Staatlichen Verwaltungen, Firmen und Privaten in Basel-Stadt gestärkt wird.

Philip Karger, Thomas Mürty, Mahir Kabakci, Lukas Faesch, Michael Hug, Raoul I. Furlano, Joël Thüring, Christoph Hochuli, Beatrice Isler, Beat von Wartburg, Semseddin Yilmaz, Balz Herter, Niggi Daniel Rechsteiner, Alex Ebi, Luca Urgese»

Wir berichten zu diesem Anzug wie folgt:

1. Ausgangslage

Erfolgreich durchgeführte Cyberangriffe im In- und Ausland mit teilweise gravierenden Konsequenzen haben gezeigt, dass nicht nur Häufigkeit und Komplexität der Cyber-Angriffe zunehmen, sondern diese auch vermehrt zielgerichtet gegen Staaten oder Unternehmen eingesetzt werden. Der Regierungsrat erachtet sowohl die Cybersicherheit sowie auch die Bekämpfung vor Cyberkriminalität als wichtige und grosse Herausforderung. Aus diesem Grund begrüsst der Regierungsrat die Stossrichtung des vorliegenden Anzugs. Eine Vermischung oder gar Zusammenlegung der beiden Themen Cyberkriminalität und Cybersicherheit wird jedoch wie in der Stellungnahme zur Motion und zum weiteren Vorgehen vom 31. August 2022 weiterhin nicht als zielführend erachtet. Verbessert werden soll aber die verwaltungsinterne Koordination, auch bei der Umsetzung der neuen – im Frühling 2023 von Bundesrat und KKJPD gutgeheissenen – Nationalen Cyberstrategie (NCS)¹ zum Schutz vor Cyberbedrohungen.

2. Cybersicherheit und Cyberkriminalität

Bei der Cybersicherheit geht es um den Schutz von Daten, Informationen oder Softwaresystemen. Im Fokus stehen alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik sowie präventive Bemühungen, um vorzubeugen, dass Privatpersonen Opfer (oder auch unwissentlich zur Täterschaft) im Cyberbereich werden. Die Kantonsverwaltung steht beim Schutz von Bürgerdaten sowie beim Schutz der eigenen kritischen Infrastrukturen in der Verantwortung.

Demgegenüber geht es bei der Bekämpfung von Cyberkriminalität um die Strafverfolgung. Mit der fortschreitenden Digitalisierung gibt es sowohl eine Verlagerung der Kriminalität in den digitalen Raum als auch ein Aufkommen von neuen Kriminalitätsformen. Die Cyberkriminellen sind ausgesprochen flexibel, anpassungsfähig und achten sehr auf gesellschaftliche Trends und Veränderungen. So stieg die Zahl der Phishing-Fälle schweizweit an, ebenso die Zahl der Ransomware-Fälle. Der Trend der Verlagerung verschiedener Kriminalitätsformen aus dem «Real Life» in die digitale Welt wird sich fortsetzen und eine bedeutende Herausforderung für Strafverfolgungsbehörden bleiben.

¹ <https://www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html>

3. Umgesetzte Massnahmen zur Stärkung der Cybersicherheit

Wie in der Stellungnahme zur Motion und zum weiteren Vorgehen vom 31. August 2022 ausgeführt, sind einzelne Forderungen bzw. Prüfungsanliegen des Vorstosses bereits umgesetzt. So wurde beispielsweise bei der Staatsanwaltschaft im Bereich der Kriminalitätsbekämpfung das Dezernat Digitale Kriminalität geschaffen, welches seit September 2020 in Betrieb ist. Im Bereich Resilienzmanagement werden die Abhängigkeiten von Systemen und anderen Dienstleistenden erhoben. Ebenso sind die wichtigsten IKT²-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 wurde eine Awareness-Kampagne zu Cyber-Risiken durchgeführt. Dies mit dem Ziel, das Sicherheitsbewusstsein der kantonalen Mitarbeitenden weiter zu erhöhen.

4. Prüfung weiterer Massnahmen

4.1 Fehlen einer übergeordneten Koordinationsstelle

Cybersicherheit und Cyberkriminalität sind komplexe und bereichsübergreifende Themen. Der hohe Koordinationsbedarf beim Querschnittsthema Cyber ist nicht nur in Basel-Stadt vorhanden und als Herausforderung identifiziert. Der Sicherheitsverbund Schweiz (SVS) hat dazu im Jahr 2021 eine «Empfehlung für die Umsetzung zur kantonalen Cyberorganisation» publiziert.³ Ein Grossteil der vom SVS empfohlenen Aufgaben sind der Abteilung IT Risk & Security der IT BS und dem Informationsicherheitsbeauftragten zugewiesen. Dazu gehören beispielsweise das Verfolgen von Cyber-Entwicklungen auf strategischer Ebene, die Beurteilung des Cyber-Sicherheitsdispositivs, die Koordination der Umsetzung der Massnahmen der Nationalen Cyberstrategie, die Beaufsichtigung von Cybervorfällen (inklusive dem Erlass von Sofortmassnahmen) sowie die Überprüfung von Standardisierungen und Regulierungen (etwa bei der Netzsicherheit). Jedoch fehlt eine übergeordnete koordinierende Zuständigkeit, welche die Schnittstellen pflegt und als zentrale Anlaufstelle innerhalb des Kantons und für die nationalen Behörden fungiert. Der Regierungsrat hat die Koordination dieser Aufgaben bereits angestossen.

4.2 Cybercrime-Meldestelle und Gefahrenkarte

Das eidgenössische Parlament hat am 29. September 2023 eine Änderung des Informationssicherheitsgesetzes (ISG) verabschiedet, mit der eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen eingeführt wird. Da dies eine vollständige Überarbeitung des 5. Kapitels des Informationssicherheitsgesetzes bedingt, erfolgt der Erlass der Ausführungsbestimmungen zu einem späteren Zeitpunkt. Die Vorlage schafft die gesetzlichen Grundlagen zur Meldepflicht für Betreiberinnen und Betreiber kritischer Infrastrukturen und definiert die Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC), welches als zentrale Meldestelle für Cyberangriffe vorgesehen ist.

4.3 Zentrale Speicherung von personenbezogenen Daten

Im Umgang mit Informationen (Sach- und Personendaten) verpflichtet das Gesetz über die Information und den Datenschutz (IDG) unter § 6, § 7, und § 8 die Verwaltung bereits heute zum Schutz der Informationen, Daten und IT-Mittel sowie dazu, organisatorische und dem Stand der Technik entsprechende technische Massnahmen umzusetzen. Aktuell erfolgt die Adressierung der gesetzlichen Forderung dezentral. Der Anzug lässt offen, was unter «sensiblen Daten» zu verstehen ist, und ob der Kanton die Speicherung sämtlicher sensibler Daten übernehmen soll. Der Regierungsrat will auf eine ausschliessliche Speicherung von sensiblen Daten durch den Kanton verzichten.

² Informations- und Kommunikationstechnologie.

³ Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation, SVS 2021: <https://www.svs-rns.ch/de/umsetzungsplan-der-kantone>.

5. Antrag

Aufgrund des obigen Ausführungen beantragen wir, den Anzug Philip Karger und Konsorten betreffend Stärkung der Cybersicherheit für Staatliche Verwaltungen, Firmen und Privaten in Basel-Stadt abzuschreiben.

Im Namen des Regierungsrates des Kantons Basel-Stadt



Dr. Conradin Cramer
Regierungspräsident



Barbara Schüpbach-Guggenbühl
Staatsschreiberin