



An den Grossen Rat

22.5216.02

JSD/P225216

Basel, 31. August 2022

Regierungsratsbeschluss vom 30. August 2022

Motion 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 01. Juni 2022 die nachstehende Motion Philip Karger und Konsorten dem Regierungsrat zur Stellungnahme 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 IT-Bereich 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 Cyber-sicherheit von Staatlichen Verwaltungen, Firmen und Privaten in Basel-Stadt gestärkt wird.

Philip Karger, Thomas Müry, 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 nehmen zu dieser Motion wie folgt Stellung:

1. Zur rechtlichen Zulässigkeit der Motion

§ 42 GO bestimmt über die Motion:

§ 42. Inhalt und Eintretensbeschluss

¹ In der Form einer Motion kann jedes Mitglied des Grossen Rates oder eine ständige Kommission den Antrag stellen, es sei der Regierungsrat zu verpflichten, dem Grossen Rat eine Vorlage zur Änderung der Verfassung oder zur Änderung eines bestehenden oder zum Erlass eines neuen Gesetzes oder eines Grossratsbeschlusses zu unterbreiten.

^{1bis} In der Form einer Motion kann zudem jedes Mitglied des Grossen Rates oder eine ständige Kommission den Antrag stellen, es sei der Regierungsrat zu verpflichten, eine Massnahme zu ergreifen. Ist der Regierungsrat für die Massnahme zuständig, so trifft er diese oder unterbreitet dem Grossen Rat den Entwurf eines Erlasses gemäss Abs. 1, mit dem die Motion umgesetzt werden kann.

² Unzulässig ist eine Motion, die auf den verfassungsrechtlichen Zuständigkeitsbereich des Regierungsrates, auf einen Einzelfallentscheid, auf einen in gesetzlich geordnetem Verfahren zu treffenden Entscheid oder einen Beschwerdeentscheid einwirken will.

³ Tritt der Rat auf die Motion ein, so gibt er dem Regierungsrat Gelegenheit, innert drei Monaten dazu Stellung zu nehmen, insbesondere zur Frage der rechtlichen Zulässigkeit des Begehrens.

Die Motion ist sowohl im Kompetenzbereich des Grossen Rates wie auch in demjenigen des Regierungsrates zulässig. Ausserhalb der verfassungsrechtlichen Kompetenzaufteilung (vgl. § 42 Abs. 2 GO) ist der betroffene Zuständigkeitsbereich somit keine Voraussetzung der rechtlichen Zulässigkeit. Die Frage nach der Zuständigkeit ist im Rahmen der inhaltlichen Umsetzung eines Motionsanliegens aber von entscheidender Bedeutung, da sie die Art der Umsetzung vorgibt. Es gilt, das Gewaltenteilungsprinzip zwischen Grosse Rat und Regierungsrat zu beachten, denn beide sind gestützt auf das Legalitätsprinzip an Erlasse gebunden, die die Entscheidungsbefugnisse auf die Staatsorgane aufteilen. Je nach betroffenem Kompetenzbereich richtet sich die Umsetzung entweder nach § 42 Abs. 1 GO oder nach § 42 Abs. 1^{bis} GO. Liegt die Motion im Zuständigkeitsbereich des Grossen Rates, wird sie mit einer Verfassungs-, Gesetzes- oder Beschlussvorlage erfüllt (§ 42 Abs. 1 GO). Eine Motion, die auf eine Materie im Kompetenzbereich des Regierungsrates zielt, wird mit einer Verordnungsänderung respektive mit einem anderen Mittel der Exekutive erfüllt (§ 42 Abs. 1^{bis} GO), oder aber dem Grossen Rat wird ein Gesetzesentwurf vorgelegt, der die Kompetenzverteilung zugunsten des Grossen Rates verändert (§ 42 Abs. 1^{bis} Satz 2 GO).

Mit der vorliegenden Motion bitten die Unterzeichnenden der Motion den Regierungsrat, die Voraussetzungen für eine Stärkung der Cybersicherheit der staatlichen Verwaltung, von Firmen und Privaten im Kanton Basel-Stadt zu schaffen. Gefordert werden diverse Massnahmen, die nachfolgend in Kursivschrift festgehalten werden:

Cybercrime-Meldestelle und Meldepflicht

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. Auf diese Informationen muss per Alert (Push) und auch auf Abruf (Pull) zugegriffen werden können.

Per Gesetz muss jede Straftat und Bedrohung sofort gemeldet werden.

Der Aufbau und Betrieb einer Cybercrime-Meldestelle dient dem präventiven Rechtsgüterschutz. Gemäss Art. 57 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101) sorgen Bund und Kantone im Rahmen ihrer Zuständigkeiten für die Sicherheit des Landes und den Schutz der Bevölkerung (Abs. 1). Sie koordinieren ihre Anstrengungen im Bereich der inneren Sicherheit (Abs. 2). Die Verhinderung von Straftaten bzw. die Gefahrenabwehr richtet sich in erster Linie nach kantonalem Polizeirecht (Diggelmann/Altwickler, in: Waldmann et al. [Hrsg.], Bundesverfassung, Basler Kommentar, Basel 2015, Art. 57 N 24 und 40; Markwalder/Lobisger, in: Niggli/Wiprächtiger, Strafrecht II, Basler Kommentar, 4. Aufl., Basel 2019, Art. 385 StGB N 8). Ferner gewährleistet die Bundesverfassung die Organisationsautonomie (Art. 47 Abs. 2 BV). Die Kantone sind unter Vorbehalt des Vorrangs des Bundesrechts berechtigt, die zur Erfüllung ihrer Aufgaben erforderlichen Organe einzusetzen und die entsprechenden Verfahren zu regeln (Belser/Massüger, in: Waldmann et al. [Hrsg.], Bundesverfassung, Basler Kommentar, Basel 2015, Art. 47 N 15). Die Regelung der Cybercrime-Prävention ist dem Bund nicht als exklusive Kompetenz zugewiesen (Art. 3 und 42 BV). Eine kantonale Cybercrime-Meldestelle ist demnach mit Bundesrecht vereinbar.

Bei der von der Motion geforderten Meldepflicht bleibt offen, welcher Zweck damit erreicht werden soll. Mit einer Meldepflicht werden die Pflichtigen dazu gezwungen, Personendaten preiszugeben. Das berührt die grundrechtlich geschützte Privatsphäre (Art. 8 EMRK; Art. 13 BV; § 11 Abs. 1 lit. g Verfassung des Kantons Basel-Stadt vom 23. März 2005 [KV; SG 111.100]). Ob ein solcher Grundrechtseingriff zulässig wäre, kann erst beurteilt werden, wenn der Zweck der Meldepflicht definiert ist. Ohne Zweckdefinition lässt sich insbesondere nicht beurteilen, ob die Grundrechtseinschränkung verhältnismässig ist oder ob der gleiche Zweck nicht möglicherweise auch mit einem auf Freiwilligkeit basierenden Melderecht erreicht werden kann.

(Art. 36 Abs. 3 BV). Es ist grundsätzlich möglich, eine grundrechtskonforme Meldepflicht zu konzipieren. Gleiches gilt für die Konzeption der Gefahrenkarte und der Information der Bevölkerung mittels Push- und Pull-Mitteilungen.

Cybersicherheitsbeauftragte

Firmen ab einer zu definierenden Grösse müssen Cybersicherheitsbeauftragte mit Kompetenzen im IT-Bereich einsetzen.

Die Organisation privater Unternehmen wird vom Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (OR; SR 220) geregelt. Die Gesetzgebung auf dem Gebiet des Zivilrechts ist Sache des Bundes (Art. 122 Abs. 1 BV). Allerdings bestimmt Art. 6 des Schweizerischen Zivilgesetzbuchs vom 10. Dezember 1907 (ZGB; SR 210), dass die Kantone in ihren öffentlich-rechtlichen Befugnissen durch das Bundeszivilrecht nicht beschränkt werden. Zum Verhältnis zwischen Bundeszivilrecht und öffentlichem Recht der Kantone führt das Bundesgericht in BGE 119 Ia 59 E. 2b aus: «Die Kantone können im öffentlichen Interesse Vorschriften aufstellen, welche die zivilrechtliche Ordnung ergänzen. Wo die Schranken der expansiven Kraft des öffentlichen Rechts liegen und welche zivilrechtlichen Vorschriften eine abschliessende Ordnung darstellen und Modifikationen durch Bestimmungen des kantonalen öffentlichen Rechts ausschliessen, lässt sich nicht in allgemeiner Form umschreiben. Nach der Rechtsprechung des Bundesgerichts ist der Erlass öffentlichrechtlicher kantonalen Vorschriften in einem vom Bundeszivilrecht geregelten Bereich gestützt auf Art. 6 ZGB zulässig, [1] sofern der Bundesgesetzgeber nicht eine abschliessende Ordnung geschaffen hat, [2] die kantonalen Bestimmungen einem schutzwürdigen öffentlichen Interesse entsprechen und [3] nicht gegen Sinn und Geist des Bundeszivilrechts verstossen [Rechtsprechungshinweise].» Es ist fraglich, ob eine Verpflichtung von privaten Unternehmen, einen Cybersicherheitsbeauftragten mit Kompetenzen im IT-Bereich einzusetzen, diesen Erfordernissen genügt. Zum einen hat der Bundesgesetzgeber die Organisation privater Unternehmen ausführlich geregelt, sodass möglicherweise eine abschliessende Ordnung vorliegt. Zum anderen ist nicht ersichtlich, inwiefern die Bedrohung oder Schädigung von Unternehmen durch Cyber-Ereignisse ein hinreichendes öffentliches Interesse darstellen. Es ist primär Aufgabe der Unternehmen, sich vor diesen Gefahren zu schützen. Zu einem anderen Schluss könnte man eventuell bei Unternehmen systemrelevanter Branchen (Energiesektor, Banken etc.) gelangen. Die Pflicht, Mitarbeiter mit einem bestimmten Kompetenzprofil einzusetzen, greift zudem in die Wirtschaftsfreiheit (Art. 27 BV) der Unternehmen ein. Grundrechtseinschränkungen bedürfen einer gesetzlichen Grundlage (Art. 36 Abs. 1 BV). Sie müssen durch ein öffentliches Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt (Art. 36 Abs. 2 BV) sowie verhältnismässig sein (Art. 36 Abs. 3 BV). Gerade beim letztgenannten Erfordernis sind Zweifel angebracht: Die Einführung eines Cybersicherheitsbeauftragten wird als isolierte Massnahme kein taugliches Mittel zur Gewährleistung der Cybersicherheit eines Unternehmens sein. Es bestehen deshalb bezüglich der Vereinbarkeit dieser Motionsforderung mit Bundesrecht Zweifel.

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 gemacht und gestärkt werden. Es braucht eine Sensibilisierung im Umgang mit der Freigabe persönlicher- und Kundendaten.

Mit dieser Forderung ist die Gefahrenabwehr angesprochen, weshalb auf die Ausführungen zur rechtlichen Zulässigkeit der Meldestelle verwiesen wird. Awareness-Kampagnen sind folglich als Massnahmen anzusehen, die (auch) in die Kompetenz der Kantone fallen.

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 viele Firmen, Bürgerinnen und Bürger nehmen die Cyberkriminalität nicht ernst genug.

Diese Forderung beschlägt erneut die Prävention von Cyberkriminalität. Bezüglich der Zuständigkeit des Kantons wird daher auf die Ausführungen zur rechtlichen Zulässigkeit der Meldestelle verwiesen.

Personenbezogene 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.

Es bleibt offen, was der Motionär unter «sensiblen Daten» versteht und ob gefordert wird, dass der Kanton die Speicherung sämtlicher sensibler Daten übernimmt.

Es sei immerhin darauf hingewiesen, dass mit einer ausschliesslichen Speicherung der sensiblen Daten durch den Kanton diese Aufgabe den Privaten entzogen und jeder Wettbewerb ausgeschaltet würde. Es würde damit ein staatliches Monopol errichtet. Das ist ein schwerer Eingriff in die Wirtschaftsfreiheit (Art. 27 BV; § 11 Abs. 1 lit. s KV). Die Kantone sind grundsätzlich befugt, neue Monopole einzuführen, sofern dies durch ein zulässiges öffentliches Interesse gerechtfertigt und verhältnismässig ist (BGE 143 I 388 E. 2.1). Die Kantonsverfassung gibt dem Gesetzgeber die Möglichkeit, im Rahmen der Wirtschaftsfreiheit durch Gesetz Monopole zu errichten (§ 38 Abs. 5 KV). Es ist aber fraglich, ob es ein hinreichendes öffentliches Interesse für ein solches Monopol gäbe (Art. 36 Abs. 2 i.i. BV). Nicht ersichtlich ist zudem, inwiefern dadurch Grundrechte Dritter geschützt würden (Art. 36 Abs. 2 i.f. BV). Im Gegenteil: Das Speichermopol würde auch in den Schutz der Privatsphäre eingreifen (Art. 13 BV; § 11 Abs. 1 lit. g KV). Und schliesslich gibt es Bedenken hinsichtlich der Verhältnismässigkeit (Art. 36 Abs. 3 BV).

Aufbau eines Kompetenzzentrums Cybercrime

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

Der Aufbau eines kantonalen Kompetenzzentrums im Bereich Cybercrime beschlägt die Organisation der Strafbehörden. Die Straftaten des Bundesrechts werden grundsätzlich von den kantonalen Strafbehörden verfolgt (Art. 22 der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 [Strafprozessordnung, StPO; SR 312.0]). Die Kantone bestimmen ihre Strafbehörden und deren Bezeichnung (Art. 14 Abs. 1 StPO). Der Kanton darf folglich ein solches Kompetenzzentrum aufbauen.

Mit der Motion werden vom Regierungsrat Massnahmen sowie – soweit erforderlich – die Ausarbeitung eines Gesetzesentwurfes beantragt. Der Erlass von Gesetzesbestimmungen fällt in die Zuständigkeit des Grossen Rates. Soweit Massnahmen verlangt werden, fallen diese nicht in den verfassungsrechtlichen Zuständigkeitsbereich des Regierungsrates. Sie beziehen sich auch nicht auf einen Einzelfallentscheid, auf einen in gesetzlich geordnetem Verfahren zu treffenden Entscheid oder einen Beschwerdeentscheid.

Die Motion ist aufgrund dieser Erwägungen als rechtlich zulässig anzusehen.

2. Inhaltliche Stellungnahme zur Motion

2.1 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. Zum anderen ist die Cybersicherheit im Sinne der behördlichen Verantwortung (Schutz von Bürgerdaten) sowie des behördlichen Selbstschutzes (Schutz kritischer Infrastrukturen) ein wichtiges Thema. Der Verlust oder Missbrauch von Daten kann massive Schäden sowohl bei Individuen als auch Firmen und Verwaltung anrichten. Deshalb ist eine stringente und ganzheitliche Strategie bezüglich Cybersicherheit entscheidend.

Demgegenüber geht es bei der Bekämpfung von *Cyberkriminalität* um die Strafverfolgung. Die Kriminalitätsformen verändern sich und die Kriminalität verlagert sich immer mehr in den digitalen Raum. 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 zu der Herausforderung für Strafverfolgungsbehörden in den nächsten Jahren werden. Der Auftrag zur Bekämpfung von Cyberkriminalität liegt beim Dezernat Digitale Kriminalität (DDK) der Staatsanwaltschaft Basel-Stadt. Das DDK gewährleistet die Strafverfolgung im Kanton Basel-Stadt bei Cyber-Delikten und unterstützt die anderen Dezernate der Kriminalpolizei sowie sämtliche Abteilungen der Staatsanwaltschaft in Fällen mit technischem oder Cyber-Bezug.

Der Regierungsrat erachtet sowohl die Cybersicherheit sowie auch die Bekämpfung von Cyberkriminalität als wichtige und grosse Herausforderung. Aus diesem Grund begrüsst der Regierungsrat die Stossrichtung der vorliegenden Motion. Eine Vermischung oder gar Zusammenlegung der beiden Themen Cyberkriminalität und Cybersicherheit wird jedoch als nicht zielführend erachtet.

2.2 Zu den einzelnen Motionsbegehren

Der Regierungsrat geht mit den Motionären einig, dass die Cybersicherheit von staatlichen Verwaltungen, Firmen und Privaten in Basel-Stadt und die Bekämpfung der Cyberkriminalität eine hohe Priorität verdienen. Einige der Motionsbegehren sind – zumindest teilweise – bereits umgesetzt oder in Planung, andere bedürfen einer vertieften Prüfung oder – aufgrund ihrer sehr offenen Formulierung – einer Präzisierung. Die folgenden Ausführungen geben eine Übersicht über die Einschätzung der einzelnen Forderungen.

2.2.1 Cybercrime-Meldestelle, Meldepflicht und Gefahrenkarte

Der Regierungsrat ist bereit, den Aufbau einer Cybercrime-Meldestelle zu prüfen. Insbesondere müsste geklärt werden, welchen Zweck die Meldepflicht erfüllen soll und ob eine gesetzliche Pflicht tatsächlich zielführender ist als ein freiwilliges Melderecht.

In der Schweiz existieren sowohl auf Bundesebene als auch in einzelnen Kantonen (beispielsweise Zürich) bereits Cybercrime-Meldestellen. So bietet das Nationale Zentrum für Cybersicherheit (NCSC) auf seiner Homepage nicht nur eine Vielzahl von Informationen für Privatpersonen und Unternehmen, sondern fordert auch zur Meldung von Ereignissen auf. In Basel wird es ab Ende Jahr 2022 für Bürgerinnen und Bürger möglich sein, via Suisse ePolice selbständig Strafanzeigen im Bereich Cybercrime (ausgewählte Delikte) zu erfassen, dieses Meldeverfahren könnte wiederum Basis für eine Gefahrenkarte fungieren.

Die Machbarkeit einer Gefahrenkarte, wie sie die Motionäre sie fordern, wird bereits in einem Pilotprojekt im Bereich des behördlichen Selbstschutzes geprüft. Bis Ende 2023 sollen unter anderem

Vorbereitungsarbeiten für eine umfassende und in die nationalen Programme eingebettete «Cyberstrategie» geleistet werden. Im Zusammenhang mit einer Cybergefährdungskarte für den Kanton muss vertieft geprüft werden, welchen Umfang die Gefahrenkarte aufweisen soll und auf Basis welcher Daten diese erstellt werden könnte.

2.2.2 Cybersicherheitsbeauftragte

In Bezug auf die Forderung, dass Firmen ab einer zu definierenden Grösse Cybersicherheitsbeauftragte mit Kompetenzen im IT-Bereich einsetzen müssen, sind grundsätzliche Fragen zu klären. Wie in Kapitel 1 (zur rechtlichen Zulässigkeit der Motion) dargelegt, müsste sorgfältig darauf geachtet werden, dass eine entsprechende Massnahme nicht in die Gesetzgebungskompetenz des Bundes oder unzulässig in die Wirtschaftsfreiheit der betroffenen Unternehmen eingreift. Der Verpflichtung von privaten Unternehmen, einen Cybersicherheitsbeauftragten oder einen Cybersicherheitsbeauftragten mit Kompetenzen im IT-Bereich einzusetzen, steht der Regierungsrat derzeit deshalb sehr kritisch gegenüber.

2.2.3 Awareness-Kampagnen

Im Bereich der Prävention sensibilisiert das Ressort Kriminalprävention der Kantonspolizei Basel-Stadt die Bevölkerung bereits heute mit Kampagnen und Einzelberatungen rund um die Themen Cybersicherheit und -crime. Die gesamte Präventionsarbeit erfolgt in enger Abstimmung mit der nationalen Austauschgruppe Cybercrimeprävention und weiteren Akteuren. Sie wird fortlaufend an die äusserst dynamische Entwicklung des Deliktfelds angepasst. Die polizeilichen Präventionsstellen werden das Thema weiter aktiv bewirtschaften.

Für Mitarbeiterinnen und Mitarbeiter der kantonalen Verwaltung wird bereits periodisch eine kantonale Awareness-Kampagne unter der Leitung des kantonalen Informations-Sicherheitsbeauftragten Basel-Stadt durchgeführt – mit dem Ziel, die Sensibilität im Umgang mit Daten, Informationen und IT-Mitteln zu steigern und die Eintrittswahrscheinlichkeit von schädigenden Ereignissen zu senken. In der Rolle des kantonalen Informationssicherheitsbeauftragten (ISB) und der Abteilung Risk & Security (FD/IT BS) werden kantonale Belange der Cybersicherheit ebenfalls bereits adressiert.

2.2.4 Staatliche Aufgaben und Angebote

Generell ist die Sensibilisierung für Selbstverantwortung und Eigenschutz ein zentraler Pfeiler der Cybersicherheit. Während es klar Aufgabe des Staates ist, innerhalb der eigenen Strukturen und Organisationseinheiten für Cybersicherheit zu sorgen und die entsprechenden Ressourcenfragen zu klären, ist die offen formulierte Motionsforderung nach staatlichen Aufgaben und Angeboten sorgfältig zu prüfen und zu präzisieren, wo staatliches Engagement unabdingbar ist und wo private Anbieter konkurriert würden. Zudem ist wiederum eine differenzierte Betrachtungsweise und eine Trennung von Cybersicherheit einerseits und Cyberkriminalität anderseits notwendig.

2.2.5 Personenbezogene Daten

Im Umgang mit personenbezogenen Daten verpflichtet das Gesetz über die Information und den Datenschutz (IDG) unter §6 und §8 die Verwaltung bereits heute zum Schutz der Daten, Informationen und IT-Mittel und dazu, organisatorische sowie dem Stand der Technik entsprechende technische Massnahmen umzusetzen. Aktuell geschieht die Adressierung der gesetzlichen Forderung dezentral. Die Motionäre lassen offen, was unter «sensiblen Daten» zu verstehen ist und ob gefordert wird, dass der Kanton die Speicherung sämtlicher sensibler Daten übernimmt. Inwiefern eine Speicherung von entsprechend klassifizierten und schützenswerten Daten in den Rechenzentren der kantonalen Verwaltung sinnvoll sein kann, ist der Regierungsrat bereit vertieft zu prüfen, weist jedoch darauf hin, dass eine ausschliessliche Speicherung der sensiblen Daten durch den Kanton ein staatliches Monopol darstellen würde und entsprechend private Anbieter verdrängen würde.

2.2.6 Aufbau eines Kompetenzzentrums Cybercrime

Der Regierungsrat ist bereit den Aufbau eines Kompetenzzentrums Cybercrime vertieft zu prüfen. Zentral ist, dass im Vorfeld die genauen Aufgaben und Verantwortlichkeiten eines solchen Zentrums detailliert bestimmt werden (Systemabgrenzung, detaillierter Anforderungs- und Aufgabenkatalog) und das bereits vorhandene Wissen eingebunden wird. Diese Zieldefinition muss auch Klarheit dahingehend bringen, welcher Skills-Mix in einem Cybercrime-Kompetenzzentrum benötigt wird.

2.3 Schlussfolgerungen

Der Regierungsrat begrüsst wie eingangs erwähnt die Stossrichtung der Motion, sieht aber zugleich massgeblichen inhaltlichen und juristischen Klärungsbedarf sowie den Bedarf nach sorgfältiger Analyse, wie weit das staatliche Engagement in diesem Bereich gehen soll und inwiefern die Zusammenarbeit mit privaten, nationalen oder ausserkantonalen Partnern effizient und zielführend gestaltet werden kann. Der Regierungsrat ist bereit, diese Fragen und die mögliche Umsetzung der Massnahmen im Rahmen einer Anzugsbeantwortung vertieft zu prüfen.

3. Antrag

Aus diesen Gründen beantragen wir, die Motion Philip Karger und Konsorten betreffend Stärkung der Cybersicherheit für Staatliche Verwaltungen, Firmen und Privaten in Basel-Stadt dem Regierungsrat als Anzug zu überweisen.

Im Namen des Regierungsrates des Kantons Basel-Stadt



Beat Jans
Regierungspräsident



Barbara Schüpbach-Guggenbühl
Staatsschreiberin