Landeskanzlei
Rathausstrasse 2
4410 Liestal
T 061 552 50 06
landeskanzlei@bl.ch
www.bl.ch

BASEL LANDSCHAFT
REGIERUNGSRAT

Regierungsrat, Rathausstrasse 2, 4410 Liestal

Sicherheitsverbund Schweiz
Maulbeerstrasse 9
3003 Bern
Per Mail:
ncsc@gs-efd.admin.ch

Liestal, 25. Oktober 2022

**Konsultationsantwort**
**Review der Nationalen Cyberstrategie NCS 2023**

Sehr geehrte Damen und Herren

Vielen Dank für die Gelegenheit zur Stellungnahme. Wir sind mit der vorgeschlagenen Strategie grundsätzlich einverstanden, insbesondere weisen wir darauf hin, dass wir an der Ausarbeitung beteiligt waren.

Wir stellen fest, dass die strategischen Ziele im Bereich «effektive Strafverfolgung» und die dort definierten Massnahmen M13 bis M15 stark auf die polizeiliche Ebene fokussieren und die Aufgaben der Staatsanwaltschaft nur am Rande behandeln. Die Sicht und die Bedürfnisse der Staatsanwaltschaft werden in der Cyberstrategie 2023 zu wenig berücksichtigt.

Wir begrüssen den Ansatz, keinen Verfallstermin zu setzen, sondern stattdessen gemäss Kapitel 4 die Strategie nach 5 Jahren zu überprüfen und anzupassen. In den einzelnen Massnahmen werden die zentralen Akteure aufgeführt. Diese sind nicht immer vollständig aufgeführt. Wo es möglich ist, sollten die konkreten Verantwortlichkeiten festgehalten werden. Die Nationale Cyberstrategie ist ein wichtiges Instrument des Bundes, enthält aber auch Aussagen über den Rest der Schweiz. Entsprechend sollte auch ein Aufruf darin festgehalten werden, dass analog dazu auch die Kantone, Gemeinden und Institutionen der Wirtschaft sowie NGO entsprechende Massnahmen ergreifen sollen.

Im vorgelegten Entwurf ist keine konkrete Umsetzungsplanung ersichtlich. Eine solche sollte noch aufgenommen werden.

Zu den Massnahmen haben wir folgende Anmerkungen:

***Massnahme M13 (*Ausbau der Zusammenarbeit der Strafverfolgungsbehörden)**

Die über Cyber-CASE (Stufe Staatsanwaltschaften; Pendant zum polizeilichen System NEDIK) bestehende Koordinations- und Kooperationsplattform wird derzeit noch nicht genutzt, da mangels eines ganzheitlichen Lagebilds sowie fehlender justizieller Fallübersicht eine Koordinierung der

Fallbearbeitung sowie eine Triage noch nicht möglich sind. Hier gibt es noch auszuschöpfendes Potential. Zu beachten ist, dass sich die Zusammenarbeit zwischen Bund und Kantonen nicht auf die polizeiliche Ebene (NEDIK) beschränken darf.

Die Kantone sind auf polizeilicher Ebene ausserhalb des Verbunds «PICSEL» derzeit noch nicht in der Lage, Querbezüge zu erkennen oder Fallgruppen (gleiche Täterschaft in verschiedenen angezeigten Sachverhalten) auf kantonaler Ebene zu bilden bzw. eine Koordination auf Bundesebene sicherzustellen. Dies wäre die Grundvoraussetzung, um effiziente Strafverfahren auf der Ebene der Staatsanwaltschaft zu führen. Diesbezüglich besteht noch Handlungsbedarf.

Eine regionale Bündelung der Kompetenzen hat keine Änderung an der Voraussetzung der ressourcen-intensiven Bekämpfung von Cyber-Kriminalität zur Folge. Die zur Bekämpfung von Cyber-Kriminalität erforderlichen Ressourcen müssen ausgebaut werden. Ob dies kantonal oder in Zentren geschieht, hat keine Auswirkungen auf den exponentiellen Anstieg dieser Kriminalitätsform und damit auf den stetig steigenden Ressourcenbedarf der Strafverfolgungsbehörden. Im Zuge der Digitalisierung nimmt die Anzahl der Berufsabschlüsse im digitalen Bereich zu, weshalb sich die Problematik der zu beschaffenden Fachkompetenzen zunehmend entspannen dürfte.

***Massnahme M14 (Fallübersicht)***

Ein Lagebild über Cyber-Kriminalität in Echtzeit ist vor allem für die Präventionsarbeit der Polizei sinnvoll. Durch die Information sowie Warnung der Bevölkerung vor gewissen Phänomenen können weitere Delikte verhindert werden. Für die eigentliche Strafverfolgung reicht jedoch ein Lagebild mit operativen Handlungsempfehlungen nicht aus. Hierfür wird eine nationale Verfahrensübersicht – grundsätzlich auf Ebene der Staatsanwaltschaft – zur Fall-Koordination sowie eine nationale Datenbank mit (Meta-)Daten zu den einzelnen Strafanzeigen im Bereich der Cyber-Kriminalität (z.B. täterische IP-Adressen, E-Mail-Adressen, Telefonnummern, Krypto-Wallet-Adressen, Webseiten etc.) wie sie bereits teilweise durch das Westschweizer Polizeikonkordat in der Form von «PICSEL» aufgebaut und in diesem Konkordat – jedoch nicht für sämtliche Phänomenbereiche – auch im Einsatz ist. Wir empfehlen eine zeitnahe Schaffung und Umsetzung der gesetzlichen Grundlagen für einen Informationsaustausch auf Bundesebene (Kanton-Kanton sowie Kantone-Bund), vorzugsweise auf Rechtsetzungsebene Bund (z.B. StPO) alternativ auf Konkordatsebene. Im Weiteren empfehlen wir den Aufbau einer nationalen Datenbank «Verfahrensübersicht» (Stufe Staatsanwaltschaft) und einer nationalen Datenbank «PICSEL» (Stufe Polizeiebene), an denen sämtliche Kantone sowie der Bund beteiligt sind. Im Anschluss an die mit «PICSEL» gesammelten praktischen Erfahrungen ist auf Grundlage dieser Erkenntnisse das Pflichtenheft für eine optimale gesamtschweizerische Software-Nachfolgelösung zu definieren und zu beschaffen.

Im Weiteren fordern wir, dass Meldungen über Ereignisse oder Anzeigen bei einer einzigen Stelle eingehen, die danach die Triage vornimmt. Momentan haben Bürgerinnen und Bürger verschiedene Meldemöglichkeiten.

***Massnahme M15 (Ausbildung der Strafverfolgungsbehörden)***

Die Polizei sowie die Fachhochschulen bieten ein relativ vielfältiges Angebot an Ausbildungen im Bereich Cybercrime an. An der Polizeischule Hitzkirch liegt der Fokus derzeit noch auf den klassischen Ausbildungsmodulen. Hier besteht noch Potential für eine Ausweitung im Bereich der Cyberkriminalität.

Für die Mitarbeitenden der Staatsanwaltschaft hat sich das Kursangebot in den vergangenen vier Jahren nicht erweitert. Wir regen an, dieses Kursangebot im Bereich der Cyberkriminalität auszubauen.

Aktuell fehlt eine Koordination zwischen den polizeilichen Weiterbildungsangeboten und den staatsanwaltschaftlichen Fachkursen. Wir würden eine Absprache oder idealerweise auch eine gegenseitige Beteiligung an den Ausbildungen der Polizei und Staatsanwaltschaft begrüssen.

***Weitere Bemerkungen***

- Für alle Verweise und Referenzen in der Nationalen Cyberstrategie sollten konsequent die Quellen und wo möglich die Links und das Datum angegeben werden.
- Das Thema der proaktiven Vorbereitung im Rahmen des Aufbaus und Betriebs der IT sollte mehr Beachtung finden in der Nationalen Cyberstrategie. Im Konsultationsentwurf sind nur Massnahmen zur Reaktion auf Ereignisse definiert.
- Das Thema «internet of things» sollte ergänzt werden mit Maschinensteuerungen (ICS) (Thema «nicht klassische Technologien»). Analog zur Telefonie werden immer mehr Bereiche der Technik (Gebäudesteuerung, Fahrzeuge, Maschinen usw.) durch digitale Sensoren, Industrie-Steuerungssysteme und die Vernetzung mit Kommunikationsnetzen bestimmt. Diese Technologien werden heute meistens ausserhalb der klassischen IT-Abteilungen gemanagt, von den Gerätelieferanten bestimmt, und es fehlen Vorgaben sowie Sicherheitsstandards. Das Thema wird in der Nationalen Cyberstrategie nicht explizit adressiert. Wir beantragen, eine zusätzliche Massnahme zu definieren mit der Verpflichtung, Verantwortlichkeiten, Prozesse und die Sicherheit zu regeln sowie Sicherheitsstandards im Bereich «internet of things» festzulegen.
- Das Thema «Quantumtechnologien» sollte auch in der Strategie aufgenommen werden. Dies könnte in der Massnahme M4 oder M6 geschehen.
- Auf Seite 7 wird die Ernennung einer Person für die Koordination der Aufgaben mit Bezug zur Cybersicherheit postuliert. In den Massnahmen findet dies aber keinen Niederschlag, wir bitten Sie, dies zu prüfen.
- In Kapitel 1.3.2. wird festgehalten: «Die Zusammenarbeit mit dem Bund wird durch den SVS koordiniert und gefördert.». Wir fordern, dass das Nationale Zentrum für Cybersicherheit NCSC auch eingebunden wird und der Satz ergänzt wird: «…und gefördert in Zusammenarbeit mit dem NCSC.»
- Auf Seite 8 werden wenig konkrete Ziele formuliert: Ziel 1: «Die Bevölkerung kann Cyberrisiken einschätzen und gewinnt dadurch Vertrauen in die Nutzung digitaler Dienstleistungen.» / Ziel 2: «Die Schweiz setzt flächendeckend Massnahmen zur Stärkung der Cyberresilienz ein.». Wir fordern hier eine konkretere Formulierung und die Definition von expliziten Massnahmen und Verantwortlichkeiten zur Befähigung von Bevölkerung und Wirtschaft.
- Massnahme M3 (Bedrohungslage): Wir bitten Sie zu prüfen, ob auch kleine Organisationen genügend Unterstützung erhalten.
- Kap. 3.2 (Massnahmen…): Erster Abschnitt, letzter Satz: «(…) gilt es für die Behörden, dass sie ihre eigenen Dienstleistungen gegenüber Cyberbedrohungen schützen.». Wir bitten Sie zu prüfen, den Begriff «Behörden» durch den weiteren Begriff «Organisationen» zu ersetzen.
- Massnahme M11 (Krisenmanagement): Hier vermissen wir Ausführungen zur Notfallvorsorge inklusive Backups, Tests usw.

- Kapitel 4 (Umsetzung der Strategie), Seite 29: Wir bitten Sie zu prüfen, ob ein international anerkannter Sicherheitsstandard festgelegt werden kann. Im Weiteren gehören unseres Erachtens Ausführungen zu Sensibilisierungskampagnen und Schulungen in dieses Kapitel.

Freundliche Grüsse

Kathrin Schweizer
Regierungspräsidentin

Elisabeth Heer Dietrich
Landschreiberin