Kanton St.Gallen
Sicherheits- und Justizdepartement

Generalsekretariat

St.Galler Strategie zum Schutz vor Cyber-Risiken

von der Regierung genehmigt am 28. April 2020

Inhaltsverzeichnis

1 Warum eine St.Galler Strategie zum Schutz vor Cyber-Risiken?

Die Schweiz befindet sich mitten im Digitalisierungsprozess. Dieser Prozess eröffnet grosse Chancen, birgt aber auch Risiken. Die wachsende Digitalisierung des Alltags[1] macht die Schweiz zunehmend abhängiger und damit verwundbarer gegenüber Störungen, Ausfällen und Missbräuchen dieser Technologien. Die rasante technologische Entwicklung, die immer stärkere Vernetzung und – im Fall von kriminellen Aktivitäten – die heterogene Täterschaft, die immer professioneller wird, bergen grosse Risiken für Staat, Gesellschaft und Wirtschaft. Zeitliche und räumliche Einschränkungen für Cyber-Angriffe gibt es kaum. Sie überschreiten territoriale Grenzen und dies in einem hochdynamischen Umfeld mit kurzen Innovationszyklen.

Noch nie waren Staat, Gesellschaft und Wirtschaft so vernetzt und so transparent wie heute – und noch nie so angreifbar. Alltägliche Produkte, aber auch Bauteile, Industrieanlagen, Fertigungsstrecken usw. sind miteinander vernetzt und kommunizieren. Alles was vernetzt ist – sei es in Gesundheit, Umweltschutz, Raumplanung, Verkehr, Wirtschaft und Arbeit, Land- und Waldwirtschaft, Versorgung und Entsorgung oder Sicherheit und Ordnung usw. –, ist angreifbar. Für Angreifer ist es mitunter ein Leichtes, sich Zugriff zu verschaffen, wenn all die vernetzten Geräte nicht «by design» vor solchen Angriffen geschützt sind. Nicht nur Personalcomputer (PC) müssen geschützt sein – der Schutz vor Cyber-Risiken ist viel umfassender.

Neben gezielten und vorsätzlichen Cyber-Angriffen (Cyber-Kriminalität, Cyber-Spionage, Cyber-Sabotage und -Terrorismus, Desinformation und Propaganda, Cyber in Konflikten) können auch menschliches Fehlverhalten und technische Ausfälle zu Schäden im Cyber-Raum[2] oder in der physischen Umwelt führen.[3]

Der Kanton St.Gallen nutzt die Chancen der Digitalisierung und stellt sich gleichzeitig den damit einhergehenden Herausforderungen. Er positioniert sich so, dass ein effektiver Schutz vor Cyber-Risiken den ganzen Kanton, die gesamte Staatsverwaltung[4], die Organisationen mit kantonaler Beteiligung sowie die Kritischen Infrastrukturen umfasst.

Der Schutz vor Cyber-Risiken ist eine Querschnitts- und Verbundsaufgabe, die nur gemeinsam zu erfüllen ist. Staat, Wirtschaft und Bevölkerung tragen eine gemeinsame Verantwortung und alle Akteure sind angehalten, mit ihrem Verhalten und ihren Massnahmen dafür zu sorgen, dass das Wohl der Gesellschaft und die Widerstandsfähigkeit gegenüber Cyber-Risiken gewahrt bleiben. Der Kanton St.Gallen will dazu seinen Beitrag leisten.

Der Kanton St.Gallen ist als Teil der Schweizerischen Eidgenossenschaft auch Teil der nationalen Cyber-Schutz-Strategien.[5] Dennoch braucht der Kanton St.Gallen eine eigene Strategie zum

---

1 Stichworte: smart government, smart home, smart building, smart city, Internet of Things [IoT], Industrie 4.0.

2 Cyber-Raum ist gemäss der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022 (nachfolgend abgekürzt NCS II), S. 31 (abrufbar unter https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html) die «Gesamtheit der Informations- und Kommunikationsinfrastrukturen (Hard- und Software), die untereinander Daten austauschen, diese erfassen, speichern, verarbeiten oder in (physische) Aktionen umwandeln, und der dadurch ermöglichten Interaktionen zwischen Personen, Organisationen und Staaten».

3 Definition der Cyber-Bedrohungslage gemäss NCS II (vgl. im Detail NCS II, S. 3ff.).

4 Staatsverwaltung im Sinn der Strategie sind Regierung, Departemente und Staatskanzlei sowie die ihnen nachgeordneten Behörden und Dienststellen.

5 NCS II sowie der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken vom 19. Juni 2012 (nachfolgend NCS I) (abrufbar unter https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/ncs_strategie-2012.html).

Schutz vor Cyber-Risiken, und zwar eine übergeordnete Gesamtstrategie, die alle Bereiche abdeckt. Nur so ist gewährleistet, dass der Cyber-Schutz den spezifischen Anforderungen im Kanton St.Gallen genügt. Diese Cyber-Schutz-Strategie fokussiert auf die Belange des Kantons unter Berücksichtigung der Arbeiten des Bundes.

1.1 Definition Cyber-Schutz

Die nationalen Cyber-Schutz-Strategien und die Organisation des Bundes unterteilen die Aufgaben und Zuständigkeiten beim Cyber-Schutz in drei Bereiche:

– «Cyber-Sicherheit»;
– «Strafverfolgung von Cyber-Kriminalität»;
– «Cyber-Defence».

Diese Strategie fokussiert auf den Bereich «Cyber-Sicherheit».

Für den Bereich «Strafverfolgung von Cyber-Kriminalität» sind der Bund und die Kantone zuständig. Eine Klärung der Rollen und Aufgaben des Kantons bzw. der Regierung sowie strategische Vorgaben und Ziele an die Kantonspolizei und Staatsanwaltschaft sind in dieser Strategie nicht erforderlich. Zum einen ist der Begriff «Strafverfolgung» klar. Zum anderen sind die Arbeiten der Kantonspolizei und der Staatsanwaltschaft des Kantons St.Gallen sowohl auf strategischer als auch operativer Ebene weit fortgeschritten und betreffen den gesamten Bereich der «Strafverfolgung von Cyber-Kriminalität». Zu nennen sind in diesem Zusammenhang insbesondere das Kompetenzzentrum Cybercrime sowie die Zusammenarbeit und Vernetzung der Kantonspolizei und der Staatsanwaltschaft im Cyberboard und im «Netzwerk für die Ermittlungsunterstützung in der digitalen Kriminalität» (Nedik).[6] Auch sind Geltungsbereich und Ausübung der Strafrechtspflege durch die Strafverfolgungsbehörden des Bundes und der Kantone in der Schweizerischen Strafprozessordnung (SR 312.0; abgekürzt StPO) bereits geregelt. In der NCS II gibt es ein spezielles Handlungsfeld «Strafverfolgung»[7]. Die Umsetzung der in der NCS II definierten vier Massnahmen[8] sind im «Umsetzungsplan der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022»[9] enthalten. Koordination und Verantwortung liegen beim Cyberboard.

Für den Bereich «Cyber-Defence»[10] ist ausschliesslich der Bund zuständig. Daher ist dieser Bereich nicht Gegenstand der Strategie.

1.2 Zweck der Strategie

Diese Strategie befasst sich umfassend mit dem Schutz des Kantons vor Cyber-Risiken. Sie klärt in erster Linie die Rolle der Regierung beim Cyber-Schutz mit dem Fokus Cyber-Sicherheit.

Die Strategie:
– versteht Cyber-Sicherheit umfassend und ist keine IKT-Strategie[11];
– stärkt die Rolle der Regierung, indem sie als Leitlinie für das strategische und operative Handeln dient und für konsistente und vorausschauende Entscheidungen sorgt;

6 Weitere Informationen zum Cyberboard und zu Nedik in der Vorstudie, S. 13f., 18f. (Beilage RRB 2019/489).
7 Strafverfolgung von Cyber-Kriminalität ist in der NCS II ein Handlungsfeld (Handlungsfeld 7 NCS II).
8 NCS II, S. 22 ff.
9 Umsetzungsplan NCS II, S. 49 ff. (abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/56943.pdf).
10 Cyber-Defence ist neu Teil der NCS, und zwar mit einem Handlungsfeld (Handlungsfeld 8 NCS II).
11 IKT = Informations- und Kommunikationstechnologie.

– ermöglicht bzw. erleichtert die Koordination und Kooperation zwischen Departementen, Ämtern und Dritten;
– ist abgestimmt mit der NCS II sowie mit weiteren Strategien und Vorgaben des Bundes und des Kantons in benachbarten Politikbereichen.

Die Strategie soll einen wichtigen Beitrag dazu leisten, damit die Verantwortlichen im Kanton St.Gallen ihre Staatsaufgaben effizient und effektiv erfüllen können.

2 Vision

Der Kanton St.Gallen gestaltet und nutzt die Möglichkeiten der Digitalisierung. Einer «smarten Gesellschaft» steht er grundsätzlich offen gegenüber. Er unterstützt den Schutz von Bevölkerung, Wirtschaft und Staat vor Cyber-Risiken. Damit erhöht er insgesamt die Widerstandsfähigkeit der Gesellschaft. Dieser Schutz betrifft nicht ausschliesslich die IKT. Vielmehr betrifft er alle Lebensbereiche, in welche die Digitalisierung Einzug hält und die für die Funktion und das Wohlergehen des Kantons relevant sind.

3 Strategische Ziele

Die Strategie dient als Leitlinie der Regierung, die als Vorgabe gelten soll, wenn der Kanton Entscheidungen im Bereich Cyber-Schutz treffen muss. Sie definiert Ziele und Grundhaltungen, die dafür sorgen, dass der Kanton in Fragen der Cyber-Risiken konsistent und vorausschauend handelt. Die Regierung verfolgt mit dieser Strategie folgende Ziele:

Risiken erkennen, präventiv handeln
Der Kanton St.Gallen ist in der Lage, Cyber- Risiken frühzeitig zu erkennen, zu bewerten und auf diese mit angemessenen Massnahmen zu reagieren. Er ist sich bewusst, dass sich die Bedrohungslandschaft im Cyber-Raum permanent weiterentwickelt. Er ist in der Lage, sich auf neue Risiken vorzubereiten und die erforderlichen Massnahmen zu ergreifen, um möglichst präventiv einen effektiven Schutz zu erreichen.

Resilient sein
Die Widerstandsfähigkeit des Kantons St.Gallen gegenüber Cyber-Angriffen ist hoch. Kommt es zu einem Ereignis, das die kantonalen Infrastrukturen betrifft, schränkt dieses die Funktionsfähigkeit des Kantons nur in geringem Umfang ein. Die Regenerationszeit bis zur Rückkehr zum Normalbetrieb ist möglichst kurz.

Kompetent sein
Der Kanton St.Gallen schafft Bedingungen, damit alle Beteiligten und Betroffenen in der Lage sind, ihre Eigenverantwortung im Umgang mit Cyber-Risiken wahrzunehmen.

Der Kanton St.Gallen ist besorgt um eine zuverlässige und widerstandsfähige Infrastruktur, die von gut ausgebildete Fachkräften betrieben und von gut ausgebildeten Mitarbeiterinnen und Mitarbeitern genutzt wird.

Adäquat handeln
Präventives Handeln kann zum Schutz vor Cyber-Risiken unter Umständen nicht immer ausreichen. Der Kanton St.Gallen greift dann ein, wenn seine eigenen Infrastrukturen ernsthaft bedroht sind und damit das Wohl des Kantons gefährdet ist oder andere Akteure und Strukturen nicht mehr in der Lage sind, Cyber-Ereignisse selbständig zu bewältigen. Er verfügt über angemessene Mittel, um auf Bedrohungen oder Ereignisse zu reagieren und um Schaden abzuwenden

oder zu minimieren. Denn ist die öffentliche Sicherheit gefährdet, ist der Staat grundsätzlich auch ohne explizite gesetzliche Regelung berechtigt und auch verpflichtet, einzuschreiten.

Partnerschaftlich zusammenarbeiten
Der Kanton St.Gallen weiss, dass er allein Cyber-Risiken nicht bewältigen kann. Er sucht und pflegt auf Regierungs- und Verwaltungsebene den Austausch mit Ansprechpartnern auf inner- und interkantonaler sowie nationaler und internationaler Ebene.

Empfängergerecht informieren
Der Kanton St.Gallen informiert adressatengerecht, angemessen und regelmässig über den Umgang mit Cyber-Risiken. Er sensibilisiert seine Bevölkerung und seine Wirtschaft und nutzt dafür Vorarbeiten und Angebote des Bundes.

4 Grundsätze

Der Kanton St.Gallen handelt beim Schutz vor Cyber-Risiken nach folgenden Grundsätzen:

Eigenverantwortliches Handeln ins Zentrum stellen
Alle Personen und Organisationen handeln grundsätzlich eigenverantwortlich. Der Kanton wird dem Prinzip der Subsidiarität folgend beim Cyber-Schutz dann aktiv, wenn er dafür rechtlich die Verantwortung trägt oder andere Akteure nicht in der Lage sind, sich eigenverantwortlich ausreichend zu schützen und damit das Gemeinwohl des Kantons gefährdet ist.

An Regeln halten und risikoorientiert handeln
Der Kanton hält sich an die anerkannten Regeln des Cyber-Schutzes. Er orientiert sich beim Schutz vor Cyber-Risiken zudem an den Grundsätzen des Risikomanagements. Massnahmen sind risikobasiert und verhältnismässig.

Bestehende Strukturen nutzen
Der Kanton nutzt möglichst bestehende Organisationen, Strukturen und Abläufe, um den Cyber-Schutz zu gewährleisten. Er legt zusammen mit den verantwortlichen Stellen die Aufgaben und Zuständigkeiten fest. Bestehen Lücken, prüft er zusätzliche Massnahmen.

Verbindlichkeit im Bereich Cyber-Schutz erhöhen
Für die Massnahmen im Bereich des Cyber-Schutzes ist die Verbindlichkeit sicherzustellen. Bei Bedarf sind entsprechende Vorgaben zu erlassen und durchzusetzen. Dafür sind allenfalls auch Anpassungen auf Gesetzesstufe oder geeignete Beschlüsse auf Ebene der Regierung vorzusehen.

Kooperieren
Der Kanton kennt seine Partner im Kanton, in der Ostschweiz, in der Schweiz und im Ausland, die ihn beim Cyber-Schutz unterstützen können. Er pflegt dieses Netzwerk. Wo sinnvoll und zweckmässig, vereinbart der Kanton Kooperationen.

Aus einer Hand informieren und mit einer Stimme sprechen
Im Kanton gibt es zentrale Stelle für Cyber-Risiken. Diese koordiniert die Arbeiten und stellt die Verbindungen zu Partnern ausser- und innerhalb des Kantons sicher.

Ökonomisch handeln
Der Kanton erfüllt auch beim Cyber-Schutz «nur» Aufgaben, die notwendig, finanzierbar, wirtschaftlich und wirksam sind; zudem sollen sie zweckmässig sein und dem ökonomischen Prinzip

folgen. Ökonomisch handelt der Staat dabei nur, wenn er die Cyber-Risiken nicht unterschätzt, sondern richtig einschätzt.

5 Akteure ausserhalb der Staatsverwaltung

Der Cyber-Raum kennt keine Grenzen, die Angreifer können irgendwo auf der Welt sein, die Angriffe können eine Vielzahl von Opfern treffen und die Opfer können verstreut auf der ganzen Welt leben. All dies macht den Cyber-Schutz so speziell und anspruchsvoll.

Cyber-Angriffe können proaktiv nicht verhindert werden. Hingegen kann mit geeigneten Massnahmen die Widerstandsfähigkeit und Kompetenz der potenziellen Opfer gegenüber Cyber-Angriffen verbessert bzw. erhöht werden. Damit einhergehend lässt sich insgesamt die «digitale Kompetenz» der Menschen erhöhen, damit sie mit technologiebezogenem Wissen und Fähigkeiten im Umgang mit digitalen Medien, die Herausforderungen der Gesellschaft meistern können. Um die strategischen Ziele der Regierung erreichen zu können, müssen die Rollen und Aufgaben mit Bezug auf die potenziellen Opfer im Kanton (nachfolgend «Akteure» genannt) beim Cyber-Schutz geklärt sein – eine enge kantonale Sicht wäre gewiss unangebracht. Gerade beim Cyber-Schutz ist in funktionellen Räumen zu denken. Deshalb sind nachfolgend in Bezug auf die verschiedenen Akteure die Rolle und die Aufgaben der Regierung aufgeführt – dies unter Berücksichtigung der Einbettung der jeweiligen Akteure im Kontext der nationalen Cyber-Schutz-Strategien.

5.1 Bevölkerung

Definition	Alle natürlichen Personen, die im Kanton St.Gallen leben oder sich aufhalten.
Rechtsgrundlagen	Der Kanton St.Gallen ist ein freiheitlicher, demokratischer und sozialer Rechtsstaat (Art. 1 Abs. 2 der Kantonsverfassung [sGS 111.1; abgekürzt KV], in dem jede Person Verantwortung für sich selbst trägt (Art. 6 Abs. 1 KV). Der Kanton ist für die Wahrung der Sicherheit und Ordnung zuständig und trägt gegenüber der Bevölkerung eine Schutzpflicht (Art. 22 KV).
Rolle und Aufgaben der Regierung	Zum Schutz vor Cyber-Risiken gilt der Grundsatz der Eigenverantwortung: Alle Anwenderinnen und Anwender sind selbstverantwortlich für ihre Cyber-Sicherheit bei der Nutzung von Informations- und Kommunikationssystemen wie Computern, Mobiltelefonen, Tablets usw. sowie bei der Nutzung ihrer digitalisierten Umgebung (smart home usw.). Der Kanton nimmt gegenüber der Bevölkerung eine unterstützende Rolle ein. Er sorgt – unter Berücksichtigung des Angebots des Bundes – dafür, dass die Bevölkerung in der Lage ist, eigenverantwortlich zu handeln. Hier sind die Regierung und der Kanton auf übergeordneter Stufe gefordert, indem sie Angebote zum Beispiel in den Themen Bildung oder Information[12] machen oder für Ereignisfälle geeignete Krisenorganisationen vorhalten.

[12] Die Schweizerische Kriminalprävention (SKP) hat als Aufgabe die Aufklärung der Bevölkerung über kriminelle Phänomene, Präventionsmöglichkeiten und Hilfsangebote. Dazu gehört das Erstellen von Broschüren, Faltblättern und Ähnlichem zu bestimmten Themen der Kriminalprävention (z.B. Internet, digitale Sicherheit, Stalking, Zivilcourage) und für spezifische Zielgruppen wie z.B. Jugendliche oder Seniorinnen und Senioren https://www.skppsc.ch/de/downloads/warengruppe/broschueren-und-faltblaetter/.

Ausführungen der NCS	Der Schutz der Bevölkerung ist letztendlich Zweck aller NCS-Massnahmen. Die Bevölkerung ist Zielgruppe der NCS II. Durch transparente Information will die NCS dazu beitragen, der Bevölkerung einen sicheren, informierten und vertrauensvollen Umgang mit Informations- und Kommunikationstechnologien zu ermöglichen.
NCS II-Umsetzungsplan der Kantone[13] **/ Umsetzungsprojekt**	UM5 «Sensibilisierung der jungen und älteren Menschen für Cyber-Risiken»
Bemerkungen	– MELANI wurde innerhalb des Kompetenzzentrums Cyber-Sicherheit des Bundes zu einer Nationalen Anlaufstelle Cybersicherheit ausgebaut (seit 1. Januar 2020 operativ).[14]
Fazit	– Die Bevölkerung kann MELANI bzw. die Nationale Anlaufstelle Cybersicherheit als Anlaufstelle für Cyber-Sicherheit nutzen. – Ergänzend zu MELANI bzw. der Nationalen Anlaufstelle Cybersicherheit kann eine kantonale Stelle für Cyber-Sicherheitvon Vorteil sein. Die Ausgestaltung einer solchen Stelle («Stelle für die SG-Öffentlichkeit») erfolgt in einem Folgeprojekt. – Mittelfristig erhöht auch die IT-Bildungsoffensive das Wissen und damit die Resilienz der Bevölkerung und reduziert menschliches Fehlverhalten. – Die Verantwortung für das Umsetzungsprojekt UM 5 liegt auf interkantonaler Ebene. [15] Der Kanton St.Gallen ist nicht primär zuständig, profitiert aber davon.

5.2 Gemeinden

Definition	Gemeinden sind die politischen Gemeinden, die Schulgemeinden und die Ortsgemeinden (Art. 88 Abs. 1 KV). Gemeinden sind juristische Personen des öffentlichen Rechts.
Rechtsgrundlagen	Der Kanton St.Gallen ist ein freiheitlicher, demokratischer und sozialer Rechtsstaat (Art. 1 Abs. 2 KV), in dem jede Person Verantwortung für sich selbst trägt (Art. 6 Abs. 1 KV). Die Gemeindeautonomie ist nach Massgabe des kantonalen Rechts gewährleistet (Art. 50 Abs. 1 der Bundesverfassung [SR 101; abgekürzt BV]). Im Kanton St.Gallen sind die Gemeinden autonom, soweit

13 «Umsetzungsplan der Kantone» ist ein Anhang im Umsetzungsplan der NCS II, abrufbar unter https://www.svs.admin.ch/de/themen-/Cybersicherheit/Cybersicherheit-Kantone.html.

14 MELANI ist die Melde- und Analysestelle Informationssicherheit des Bundes. MELANI besteht seit dem Jahr 2004. Der Bund plant einen massiven Ausbau des Kompetenzzentrums Cybersicherheit um 67 Stellen in den nächsten drei Jahren. Dabei erhält der operative Teil, der hauptsächlich aus MELANI aufgebaut wird, zusätzlich 24 Stellen. Damit wird MELANI zur nationalen Anlaufstelle für Fragen zu Cyber-Risiken ausgebaut (zu MELANI vgl. https://www.melani.admin.ch/melani/de/home.html).

15 Die Umsetzungsverantwortung liegt bei der Schweizerischen Konferenz der kantonalen Erziehungsdirektoren (EDK) in Zusammenarbeit mit der Konferenz der kantonalen Sozialdirektorinnen und Sozialdirektoren (SODK) und der Schweizerischen Kriminalprävention (SKP) (NCS II-Umsetzungsplan der Kantone, S. 76).

	das Gesetz ihre Entscheidungsfreiheit nicht einschränkt (Art. 89 Abs. 1 KV). Der Kanton ist für die Wahrung der Sicherheit und Ordnung zuständig und trägt gegenüber den Gemeinden eine Schutzpflicht (Art. 22 KV).
Rolle und Aufgaben der Regierung	Dem Prinzip der Gemeindeautonomie folgend, sind die Gemeinden dafür verantwortlich, die ihnen gemäss Kantonsverfassung zukommenden Aufgaben selbständig nach eigenem Ermessen zu erfüllen. Daher sind sie ebenfalls eigenverantwortlich für einen ausreichenden Schutz vor Cyber-Risiken zuständig. Der Kanton greift erst dann (subsidiär) in die Selbständigkeit bzw. Autonomie der Gemeinden ein, wenn das Wohlergehen der Gesellschaft wesentlich betroffen ist und die Gemeinden nicht mehr in der Lage sind, allfällige Probleme selbständig zu lösen. So lange dies nicht erforderlich ist, hat der Kanton primär eine unterstützende Rolle.
Ausführungen der NCS	Die Gemeinden sind nicht primäre Zielgruppe von NCS I und NCS II. Die Gemeinden sind wie der Kanton Teil der Schweizerischen Eidgenossenschaft und damit auch Teil der nationalen Cyber-Schutz-Strategien.
NCS II-Umsetzungsplan der Kantone / Umsetzungsprojekt	–
Bemerkungen	– MELANI wurde innerhalb des Kompetenzzentrums Cyber-Sicherheit des Bundes zu einer Nationalen Anlaufstelle Cybersicherheit ausgebaut (seit 1. Januar 2020 operativ). – Die E-Government St.Gallen (eGovSG) ist im Bereich IKT für den Teilbereich E-Government zentral.
Fazit	– Für die Gemeinden ist neben MELANI bzw. der Nationalen Anlaufstelle Cybersicherheit keine spezielle St.Galler Anlaufstelle für Cyber-Sicherheit erforderlich. – Für Gemeinden kann eine kantonale Stelle für Cyber-Sicherheit von Vorteil sein. Die Ausgestaltung einer solchen Stelle («Stelle für die SG-Öffentlichkeit»)erfolgt in einem Folgeprojekt. – Mittelfristig erhöht auch die IT-Bildungsoffensive das Wissen und damit die Resilienz der Gemeinden und reduziert menschliches Fehlverhalten.

5.3 Wirtschaft

Definition	Alle (natürlichen und juristischen) Personen, die im Kanton St.Gallen unternehmerisch tätig sind.
Rechtsgrundlagen	Der Kanton St.Gallen ist ein freiheitlicher, demokratischer und sozialer Rechtsstaat (Art. 1 Abs. 2 KV), in dem jede Person Verantwortung für sich selbst trägt (Art. 6 Abs. 1 KV).

	Die Grundrechte sind nach Massgabe der Bundesverfassung gewährleistet, namentlich Eigentumsgarantie (Art. 2 Abs. 1 Bst. t KV) und Wirtschaftsfreiheit (Art. 2 Abs. 1 Bst. u KV). Der Kanton ist für die Wahrung der Sicherheit und Ordnung zuständig und trägt gegenüber der Wirtschaft eine Schutzpflicht (Art. 22 KV).
Rolle und Aufgaben der Regierung	Wie auch Privatpersonen sind die Akteure der Wirtschaft für Schutzmassnahmen gegen Cyber-Risiken prinzipiell selbst verantwortlich. Es gilt auch hier der Grundsatz der Eigenverantwortung. Der Kanton ist sich der Bedeutung einer Wirtschaft bewusst, die gegen Cyber-Risiken wirksam geschützt ist. Dem Subsidiaritätsprinzip folgend, wird er nur dann aktiv, wenn die Akteure der Wirtschaft nicht selbständig in der Lage sind, einen wirksamen Schutz aufrechtzuerhalten, und die öffentliche Sicherheit bedroht ist. Unter den Begriff «Wirtschaft» können auch Organisationen mit kantonaler Beteiligung subsumiert werden; bei solchen sind die Rolle und die Aufgaben der Regierung jedoch andere, vgl. Abschnitt 5.4. Unter den Begriff «Wirtschaft» können auch Träger von Kritischen Infrastrukturen subsumiert werden; bei solchen sind die Rolle und Aufgaben der Regierung jedoch andere, vgl. Abschnitt 5.5
Ausführungen NCS	Die kleinen und mittleren Unternehmen (KMU) sind Zielgruppe der NCS II.
NCS II-Umsetzungsplan der Kantone / Umsetzungsprojekt	–
Bemerkungen	– MELANI wurde innerhalb des Kompetenzzentrums Cyber-Sicherheit des Bundes zu einer Nationalen Anlaufstelle Cybersicherheit ausgebaut (seit 1. Januar 2020 operativ). – .
Fazit	– Für die Wirtschaft ist neben MELANI bzw. der Nationalen Anlaufstelle Cybersicherheit keine spezielle St.Galler Anlaufstelle Cyber-Sicherheit erforderlich. – Namentlich für KMU kann eine kantonale Stelle für Cyber-Sicherheit von Vorteil sein. Die Ausgestaltung einer solchen Stelle («Stelle für die SG-Öffentlichkeit») erfolgt in einem Folgeprojekt. – Mittelfristig erhöht auch die IT-Bildungsoffensive das Wissen und damit die Resilienz der Mitarbeitenden der Wirtschaft und reduziert menschliches Fehlverhalten.

5.4 Organisationen mit kantonaler Beteiligung

Definition	Als Organisationen mit kantonaler Beteiligung gelten die selbständigen öffentlich-rechtlichen Anstalten und die juristischen Personen des öffentlichen Rechts oder des Bundeszivilrechts, welche die Voraussetzungen von Art. 94a des Staatsverwaltungsgesetzes (sGS 140.1; abgekürzt StVG) erfüllen; sie sind im Beteiligungsspiegel aufgeführt.

	Organisationen mit kantonaler Beteiligung erfüllen ihnen übertragene kantonale Staatsaufgaben.
Rechtsgrundlagen	Die Organisationen mit kantonaler Beteiligung weisen eine eigene Rechtspersönlichkeit auf. Sie können juristische Personen des öffentlichen Rechts oder des Privatrechts sein. Es kommen die diesbetreffenden Rechtsgrundlagen zur Anwendung.
Rolle und Aufgaben der Regierung	Wie auch Privatpersonen und Akteure der Wirtschaft sind die Organisationen mit kantonaler Beteiligung für Schutzmassnahmen gegen Cyber-Risiken prinzipiell selbst verantwortlich. Es gilt auch hier der Grundsatz der Eigenverantwortung. Die Rolle und die Aufgaben der Regierung sind je nach Rechtstyp der Organisation sehr unterschiedlich. So sind die Rolle und die Aufgaben der Regierung bei den juristischen Personen des kantonalen Rechts im kantonalen Recht selbst definiert. Bei den anderen juristischen Personen gibt es keine im Privatrecht definierten spezifischen Rollen und Aufgaben der Regierung. Dies gilt im Allgemeinen, aber auch mit Bezug auf Cyber-Sicherheit. Mit Bezug auf Steuerung und Beaufsichtigung von Organisationen mit kantonaler Beteiligung (Art. 94a ff. StVG) gelten die speziellen Bestimmungen des Staatsverwaltungsgesetzes (Stichwort Public Corporate Governance [PCG], Beteiligungsstrategie).
Ausführungen der NCS	–
NCS II-Umsetzungsplan der Kantone / Umsetzungsprojekt	–
Bemerkungen	Elf Organisationen mit kantonaler Beteiligung sind Träger von Kritischen Infrastrukturen (25 Objekte) vgl. Abschnitt 5.5.
Fazit	– Für Organisationen mit kantonaler Beteiligung ist neben MELANI bzw. der Nationalen Anlaufstelle Cybersicherheit keine spezielle St.Galler Anlaufstelle für Cyber-Sicherheit erforderlich. – Für Organisationen mit kantonaler Beteiligung kann eine kantonale Stelle für Cyber-Sicherheit von Vorteil sein. Die Ausgestaltung einer solchen Stelle («Stelle für die SG-Öffentlichkeit») erfolgt in einem Folgeprojekt. – Mittelfristig erhöht auch die IT-Bildungsoffensive das Wissen und damit die Resilienz der Mitarbeitenden der Wirtschaft und reduziert das menschliche Fehlverhalten. – Die Steuerung und Beaufsichtigung erfolgen durch die Regierung. – Es sind Vorgaben und Muster für die Implementierung des Schutzes vor Cyber-Risiken bei Organisationen mit kantonaler Beteiligung zu erarbeiten (einschliesslich Meldepflicht von Vorfällen an den Kanton).

5.5 Kritische Infrastrukturen

Definition	Als Kritische Infrastrukturen (KI) gelten gemäss NCS II «Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind».
Rechtsgrundlagen	Es gibt kein spezifisches Gesetz für Kritische Infrastrukturen – weder auf Stufe Bund noch auf Stufe Kanton. Bestimmungen, die auch auf Kritische Infrastrukturen anwendbar sind, sind auf Stufe Bund in der Gesetzgebung zur Landesverteidigung (5. Kapitel der Systematischen Gesetzessammlung) enthalten. Im kantonalen Recht gibt es keine. Die Träger Kritischer Infrastrukturen können juristische Personen des öffentlichen Rechts und des Privatrechts sein. Diese Rechtsgrundlagen kommen ergänzend zur Anwendung.
Rolle und Aufgaben der Regierung	Dem Grundsatz der Eigenverantwortung folgend, ist es primär die Aufgabe der Träger der Kritischen Infrastrukturen, Schutz vor Cyber-Risiken zu gewährleisten. Aufgrund der Relevanz Kritischer Infrastrukturen für die Bevölkerung und deren Lebensgrundlagen muss der Kanton subsidiär, aber bereits präventiv die Möglichkeit haben einzuschreiten, wenn die Träger Kritischer Infrastrukturen keine oder ungenügende Vorkehrungen für den Schutz vor Cyber-Risiken treffen. Hierfür ist eine explizite gesetzliche Grundlage erforderlich.[16]
Ausführungen der NCS	Kritische Infrastrukturen haben höchste Priorität. Kritische Infrastrukturen waren schon Zielgruppe der NCS I und sind es weiterhin in der NCS II.
NCS II-Umsetzungsplan der Kantone / Umsetzungsprojekt	UM3 «Erhebungstool zur Verbesserung der IKT-Resilienz in den Kantonen» UM7 «Cyber-Übung mit kritischen Infrastrukturen im Gesundheitssektor»
Bemerkungen	– Im Inventar kritischer Infrastrukturen des Kantons St.Gallen sind aktuell 130 KI (Objekte) erfasst (Stand: Okt. 2019). – Bei 22 KI ist der Kanton Träger (zwei Departemente[17]). – Bei 25 KI ist eine Organisation mit kantonaler Beteiligung Träger (insgesamt elf Organisationen mit kantonaler Beteiligung[18]). – 83 KI haben andere Träger («Dritte»).
Fazit	– Den Kritischen Infrastrukturen steht primär MELANI als Anlaufstelle für Cyber-Sicherheit zur Verfügung.

16 Eine explizite gesetzliche Regelung ist erforderlich, um die Grundrechte (insbesondere Eigentumsgarantie [Art. 26 BV] und Wirtschaftsfreiheit [Art. 27 BV]) der Träger von Kritischen Infrastrukturen einschränken zu können (Art. 36 BV). Die Berufung auf die allgemeinen Verfassungsbestimmungen zur Sicherheit erscheint nicht nur aus juristischer, sondern v.a. auch aus demokratischer Sicht als ungenügend.

17 1 KI beim Departement des Innern und 21 KI beim Sicherheits- und Justizdepartement.

18 1 KI bei 1 Organisation im Zuständigkeitsbereich des Volkswirtschaftsdepartementes, 1 KI bei 1 Organisation im Zuständigkeitsbereich des Departementes des Innern, 4 KI bei 2 bei 2 Organisationen im Zuständigkeitsbereich des Finanzdepartementes, 8 KI bei bei 4 Organisationen im Zuständigkeitsbereich des Baudepartementes, 11 KI bei bei 3 Organisationen im Zuständigkeitsbereich des Gesundheitsdepartementes.

– Für Träger Kritischer Infrastrukturen kann eine kantonale Stelle für Cyber-Sicherheit von Vorteil sein. Die Ausgestaltung einer solchen Stelle («Stelle für die SG-Öffentlichkeit») erfolgt in einem Folgeprojekt.

– Die Zuständigkeit des Kantons und damit die Rolle und die Aufgaben der Regierung bei Kritischen Infrastrukturen, deren Träger Dritte sind, sind – einschliesslich Meldepflicht von Vorfällen an den Kanton zu klären. Dies erfolgt in einem Folgeprojekt.

– Es ist ein Gesamtkonzept, gegebenenfalls eine Strategie, zum Schutz der Kritischen Infrastrukturen unter Berücksichtigung der verschiedenen Träger zu erstellen, die auch den Cyber-Schutz betrifft. Dies erfolgt in einem Folgeprojekt.

– Für proaktives Handeln des Kantons bei Kritischen Infrastrukturen, deren Träger Dritte sind, ist die Schaffung einer gesetzlichen Grundlage zu prüfen (Art. 36 Abs. 1 BV). Dies erfolgt in einem Folgeprojekt.

– Die Umsetzungsverantwortung für die Umsetzungsprojekte der NCS II liegt auf interkantonaler bzw. Bundesebene. Der Kanton St.Gallen ist nicht primär zuständig, profitiert aber davon.

6 Staatsverwaltung

Nachfolgend sind Leitgedanken sowie Vorgaben und Ziele der Regierung zum Cyber-Schutz in der Staatsverwaltung definiert.

6.1 Vorgaben und Ziele der Regierung

Aufgrund der Komplexität des Themas Cyber-Sicherheit betreibt die Staatsverwaltung einen Single Point of Contact (SPoC) für die Staatskanzlei und die Departemente.[19]

Für die Koordination und Kooperation zwischen Departementen, Staatskanzlei, Ämtern und Dritten ist ein Single Point of Contact erforderlich.

Der Schutz vor Cyber-Risiken ist ein mehrdimensionales und sich im Fluss befindliches Querschnittsthema, das nicht nur alle Departemente und die Staatskanzlei des Kantons St.Gallen angeht, sondern die öffentliche Hand auf allen Stufen, die Privatwirtschaft und den Hochschulbereich auf nationaler und internationaler Ebene tangiert.

Die Staatsverwaltung ist gehalten, kooperative Partnerschaften einzugehen und zu pflegen.

Der Bund übernimmt beim Schutz vor Cyber-Risiken eine führende Rolle. Die vorhandenen und künftigen Arbeiten des Bundes (Nationale Cyber-Schutz-Strategien usw.[20]), des Sicherheitsverbundes Schweiz (SVS), der Konferenz der Kantonsregierungen (KdK) sowie der Fachdirektorenkonferenzen sind für die Cyber-Sicherheit wichtig; ebenso die Instrumente und Institutionen der

19 Dieser ist gleichzeitig – unter Berücksichtigung der Angebote des Bundes (MELANI, Nationale Anlaufstelle für Cyber-Risiken) – auch St.Galler Ansprechstelle für Bevölkerung, Gemeinden, Wirtschaft, Organisationen mit kantonaler Beteiligung sowie Kritische Infrastrukturen.

20 Abrufbar unter https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs.html.

Aussenbeziehungen auf Regierungs- und Verwaltungsebene[21], aber auch der Innenbeziehungen[22].
Die Mitglieder der Regierung und die Vertreterinnen und Vertreter der Staatsverwaltung nehmen in den inter- und innerkantonalen Gremien eine aktive Rolle wahr und stellen die Information auch an den SPoC sicher. Die Ausgestaltung wird im Folgeprojekt geklärt.

Im vom SVS erarbeiteten Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022 sind neun Umsetzungsprojekte aufgeführt. Mit Ausnahme des Umsetzungsprojekts 8 «Schaffung der kantonalen Organisation für Cyber-Sicherheit» liegt die Umsetzungsverantwortung nicht bei den jeweiligen Kantonen, sondern beim Bund, bei Gremien des Bundes oder bei interkantonalen Gremien.[23]
Die Arbeiten des Bundes und der interkantonalen Gremien werden für die Staatsverwaltung bestmöglich genutzt. Im Kanton St.Gallen wird eine kantonale Stelle für Cyber-Sicherheit vorgesehen.

Die Cyber-Bedrohungslage wird ausgelöst durch Cyber-Angriffe, menschliches Fehlverhalten und technische Ausfälle.[24] Der Schutz vor Cyber-Risiken umfasst nicht nur den Schutz der IT-Services[25], sondern den aller Lebensbereiche, in welche die Digitalisierung Einzug hält und die für die Funktion und das Wohlergehen des Kantons relevant sind. Alle Departemente und die Staatskanzlei sind bei der Cyber-Sicherheit – je nach Geschäftskreis höchst unterschiedlich – gefordert; letztendlich aber auch jede einzelne Mitarbeiterin und jeder einzelne Mitarbeiter.
Die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter der Staatsverwaltung für die Gefahren der digitalen Welt ist zentral. Sie wird unterstützt und regelmässig überprüft.

Oberste Priorität beim Schutz vor Cyber-Risiken haben die eigenen Kritischen Infrastrukturen. Unmittelbar sind das Sicherheits- und Justizdepartement und das Department des Innern sowie mittelbar das Volkswirtschaftsdepartment, das Finanzdepartment, das Baudepartement und das Gesundheitsdepartement betroffen. Die interdepartementale Federführung für den Schutz Kritischer Infrastrukturen liegt beim Sicherheits- und Justizdepartement.
Dem Schutz der eigenen Kritischen Infrastrukturen kommt auch bei der Cyber-Sicherheit oberste Priorität zu.

Die Möglichkeiten der Einflussnahme auf die Organisationen mit kantonaler Beteiligung sind vielfältig. Je nach Organisation ist dies möglich über ein entsprechendes Gesetz, die Eigentümerstrategie, einen Mandatsvertrag, einen Arbeitsvertrag oder über die Aktionärsverantwortung. Die interdepartementale Federführung für Organisationen mit kantonaler Beteiligung liegt beim Finanzdepartement.

---

21 Vgl. Bericht der Regierung 40.16.09 «Strategie der Aussenbeziehungen 2016», S. 9 ff.

22 Die künftige strategische Ausrichtung der Regierung ist Gegenstand des Berichts der Regierung 40.19.03 «Strategiebericht Aussenbeziehungen 2020», S. 10 f. Vgl. auch den Bericht 40.16.09 «Strategie der Aussenbeziehungen 2016».

23 UP1 «Entwicklung eines Weiterbildungskonzepts und -moduls für kantonale Verwaltungen, *Umsetzungsverantwortung:* ILCE, SBFI, Koordinationsstelle NCS und SIK; UP2 «#MISP – Malware Information Sharing Plattform von MELANI für und mit den Kantonen», *Umsetzungsverantwortung:* MELANI und die Kantone; UP3 «Erhebungstool zur Verbesserung der IKT-Resilienz in den Kantonen», *Umsetzungsverantwortung:* Kanton Basel-Stadt in Zusammenarbeit mit SVS; UP4 «Verstärkter Erfahrungsaustausch über die Schweizerische Informatikkonferenz (SIK) mit der Schaffung von Grundlagen», *Umsetzungsverantwortung:* SVS; UP5 «Sensibilisierung der jungen und älteren Menschen für Cyberrisiken», *Umsetzungsverantwortung:* EDK, SODK, SKP; UP6 «Umsetzung der Netzwerksicherheitspolicy (NSP)», *Umsetzungsverantwortung:* KdK; UP7 «Cyber-Übung mit kritischen Infrastrukturen im Gesundheitssektor», *Umsetzungsverantwortung:* Bundeskanzlei, GDK; UP9 «Aktive Kommunikation zu den Tätigkeiten der Kantone im Rahmen der NCS II», *Umsetzungsverantwortung*: SVS.

24 Definition der Cyber-Bedrohungslage gemäss NCS II (vgl. im Detail NCS II, S. 3 ff.).

25 Zuständigkeit Dienst für Informatikplanung (DIP).

Der Schutz vor Cyber-Risiken wird bestmöglich in den Organisationen mit kantonaler Beteiligung verankert. Oberste Priorität haben solche Organisationen, die gleichzeitig eine Kritische Infrastruktur darstellen bzw. umfassen.

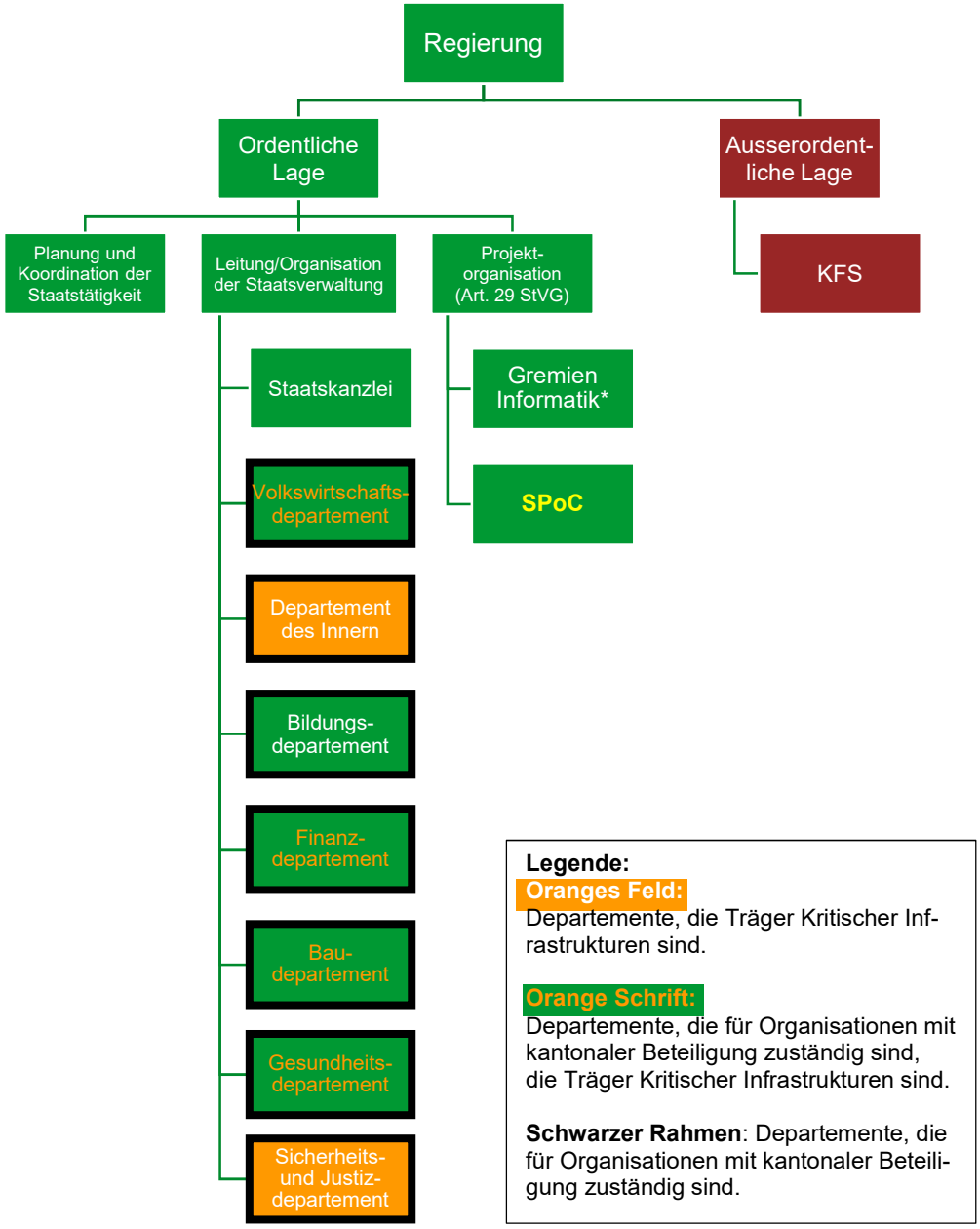
Ein wirksamer Schutz vor Cyber-Risiken ist schon in der ordentlichen Lage eine Herausforderung für die Departemente und die Staatskanzlei. Diese Aufgabe wird umso anspruchsvoller im Fall einer ausserordentlichen Lage. Der Kantonale Führungsstab (KFS) ist das Führungsinstrument der Regierung für solche Lagen, die durch gezielte und vorsätzliche Cyber-Angriffe, durch unbeabsichtigte Handlungen oder natur- und technikbedingte Ereignisse entstehen und zu Schäden im Cyber-Raum oder in der physischen Umwelt führen können.[26] Der KFS kann auch dann aktiv werden, wenn Cyber-Angriffe auf übergeordneter Ebene stattfinden und sich unmittelbar noch keine Auswirkungen im Kanton St.Gallen abzeichnen. Der KFS muss in einer ausserordentlichen Lage einsatzfähig sein und dafür sorgen, dass im Kanton St.Gallen wieder eine ordentliche Lage herrscht.

Die Führungsfähigkeit der kantonalen Behörden ist bei einem Cyber-Vorfall durch den KFS sichergestellt.

6.2 Planung und Steuerung der Regierung

Die nachfolgende Grafik gibt einen Überblick über die für die Planung und Steuerung der Regierung wesentlichen Themenfelder im Bereich Cyber-Sicherheit unter Berücksichtigung der Kritischen Infrastrukturen sowie der Organisationen mit kantonaler Beteiligung. Dabei wird zwischen ordentlicher und ausserordentlicher Lage differenziert.

[26] Beschreibung der Cyber-Bedrohungslage gemäss NCS II, S. 3 ff., S. 5.



* Gremien Informatik vgl. https://intranet.sg.ch/informatik/gremien/Seiten/default.aspx.

7 Umsetzung der Strategie

Die Umsetzung der Strategie erfolgt grundsätzlich im Rahmen der Schwerpunktplanung 2021–2031 (top–down) und unter Berücksichtigung und Miteinbezug der IT-Bildungsoffensive und der Digitalisierungsstrategie. Die in der vorliegenden Strategie in den Abschnitten 5[27] und 6[28] aufgeführten Aufgaben sind zeitlich vorzuziehen. Im Weiteren sind die bereits laufenden und neuen Projekte mit Bezug zu Cyber-Risiken und dem Schutz vor Cyber-Risiken auf Stufe Departemente und nachgeordneter Behörden und Dienststellen weiter zu planen und umzusetzen.

7.1 Cyber-Schutz in den Planungs- und Steuerungskreislauf integrieren

Der Schutz vor Cyber-Risiken ist neu explizit in den Planungs- und Steuerungskreislauf der Regierung aufzunehmen.[29] Es bietet sich an, diesen in die Schwerpunktplanung 2020–2030 aufzunehmen. Damit findet der Schutz vor Cyber-Risiken auch Eingang in die zu aktualisierenden Strategien aller Departemente und der Staatskanzlei sowie in die mittelfristige Ressourcenplanung (Aufgaben- und Finanzplan [AFP], Budget). Auch das Controlling wird mit Geschäftsbericht, Controllingbericht, Staatsrechnung und Staatszielmonitoring sichergestellt. Die Umsetzung dieser Strategie erfolgt somit in diesen Gefässen.

7.2 Aufgaben mit hohem Handlungsbedarf vorziehen

Die bereits identifizierten Aufgaben zur Unterstützung der Akteure ausserhalb der Staatsverwaltung beim Cyber-Schutz und auf interdepartementaler Ebene sind im Hinblick auf die neue Schwerpunktplanung zu konkretisieren und gegebenenfalls bereits zu realisieren. Dies gilt namentlich für:

- den Single Point of Contact für die Staatsverwaltung,
- die «Stelle für die SG-Öffentlichkeit» (Bevölkerung, Gemeinden, Organisationen mit kantonaler Beteiligung, Kritische Infrastrukturen)
- die Vorgaben und Muster für die Implementierung des Cyber-Schutzes (einschliesslich Meldepflicht) bei Organisationen mit kantonaler Beteiligung;
- das Gesamtkonzept (gegebenenfalls eine Strategie [einschliesslich Meldepflicht]) zum Schutz vor Cyber-Risiken für alle Träger Kritischer Infrastrukturen
- das Gesetzgebungsprojekt für proaktives Handeln des Kantons bei Kritischen Infrastrukturen, deren Träger Dritte sind.

7.3 Bei der Umsetzung der Strategie kooperieren

Es ist ein strategisches Ziel des Kantons, den wirksamen Schutz des Kantons St.Gallen vor Cyber-Risiken in gemeinschaftlicher Zusammenarbeit zu erreichen. Der Kanton wird daher zur Umsetzung dieser Strategie – soweit zweckmässig – mit anderen Akteuren oder Organisationen zusammenarbeiten:

- *Gemeinden:* Der Kanton St.Gallen pflegt beim Cyber-Schutz einen engen Austausch mit seinen Gemeinden und arbeitet wo nötig und zweckmässig mit diesen zusammen. Dazu nutzt er

---

27 Stelle für die SG-Öffentlichkeit; Vorgaben und Muster für die Implementierung des Schutzes vor Cyber-Risiken bei Organisationen mit kantonaler Beteiligung; Gesamtkonzept zum Schutz der Kritischen Infrastrukturen.

28 Single Point of Contact (SPoC) für die Staatsverwaltung.

29 Vgl. Konzept «Planungs- und Steuerungsinstrumente», abrufbar unter https://www.sg.ch/politik-verwaltung/regierung/planen-und-steuern.html.

die bestehenden Strukturen (eGovSG) und Kanäle, namentlich die Vereinigung St.Galler Gemeindepräsidentinnen und Gemeindepräsidenten (VSGP) mit ihren nachgelagerten acht Themenbereichen.
- *Andere Kantone:* Für den Cyber-Schutz arbeitet der Kanton St.Gallen mit anderen Kantonen zusammen. Diese Kooperation ist unkompliziert, die Kantone unterstützen sich gegenseitig. Für spezifische Themen bietet es sich an, «regionale kantonale Cluster» zu bilden, um Fragestellungen gemeinsam zu bearbeiten und bei Bedarf z.B. gegenüber dem Bund mit mehr Gewicht aufzutreten. Der Kanton St.Gallen nutzt dazu auch das Netzwerk, das durch die kantonale Koordinationsstelle für Aussenbeziehungen bereitgestellt wird.[30]
- *Interkantonale Konferenzen:* Der Kanton St.Gallen bringt Anliegen der Cyber-Sicherheit, die alle Schweizer Kantone betreffen, in die geeigneten interkantonalen Konferenzen, beispielsweise die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD), in die Ostschweizer Regierungskonferenz (ORK) oder in die Schweizerische Informatikkonferenz (SIK CSI), ein und strebt innerhalb dieser Konferenzen geeignete Lösungen an.
- *Bund:* Der Kanton St.Gallen kooperiert beim Cyber-Schutz eng mit den verantwortlichen Stellen des Bundes und partizipiert in den relevanten Bundesgremien und bei Fachveranstaltungen. Der Informations- und Meldefluss findet kontinuierlich in beide Richtungen statt.
- *Dritte/Private:* Mit Dritten wie beispielsweise Hochschulen oder Unternehmen findet regelmässig ein Informations- und Erfahrungsaustausch statt. Die jeweiligen Erwartungen wie auch die gegenseitigen Bedürfnisse sind aktiv abzuholen und beim Erreichen der strategischen Ziele zu berücksichtigen.
- *Ausland:* Die Kooperation beim Cyber-Schutz mit dem Ausland ist primär Bundesaufgabe. Der Kanton St.Gallen unterstützt – wenn aus seiner Sicht zweckmässig – den Bund bei spezifischen Fragestellungen, wenn eine Kooperation über die Landesgrenzen hinaus erforderlich ist.

8 Aktualisierung der Strategie

Die vorliegende Strategie ist auf unbestimmte Zeit gültig. Ein Schwergewicht liegt bei dieser – da ersten – Cyber-Schutz-Strategie bei der Klärung der Rolle und Aufgaben der Regierung gegen aussen. Eine Aktualisierung findet dann statt, wenn sich die Rahmenbedingungen für einen wirksamen Cyber-Schutz des Kantons St.Gallen massgeblich verändern sollten. Es obliegt dem Departement, das die Verantwortung für den SPoC übernimmt, den Zeitpunkt einer Aktualisierung zu bestimmen.

30 Vgl. Bericht der Regierung 40.16.09 «Strategie der Aussenbeziehungen 2016».