Sicherheitsverbund Schweiz
Réseau national de sécurité
Rete integrata Svizzera per la sicurezza

Jahresbericht zum Stand der Projekte im Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022

März 2021

Dieser Bericht bietet der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren regelmässig einen Überblick über den Stand der Projekte aus dem Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022. Er deckt die letzten zwölf Monate (April 2020 bis März 2021) ab und wurde vom Sicherheitsverbund Schweiz in Zusammenarbeit mit den Projektverantwortlichen verfasst.

Inhaltsverzeichnis

Überblick des Umsetzungsstands der Projekte

Handlungsfelder	Name des Projekts	Umsetzungsverantwortung	Messbare Ziele (gemäss Umsetzungsplan der Kantone)	Erreichte Meilensteine	Ausblick/Folgearbeiten
Kompetenzen- und Wissensaufbau	(1) Entwicklung eines Weiterbildungskonzepts und -moduls für kantonale Verwaltungen	Arbeitsgruppe, Leitung von Sébastien Jaquier, Leiter des *Institut de lutte contre la criminalité économique* (ILCE) der *Haute école de gestion Arc*, Neuenburg	• Erster Bericht; Ausgangslage • Ausbildungskonzept mit Zieldefinitionen nach Zielgruppen • Umfassendes, auf das Personal der kantonalen Verwaltungen zugeschnittenes Ausbildungsprogramm • Erarbeitung eines didaktischen Instruments, zum Beispiel im E-Learning-Format	• Einsetzung der Arbeitsgruppe und der Unterarbeitsgruppen • Bestandsaufnahme der in den Kantonen vorhandenen Weiterbildungen • Erstellung des Weiterbildungskonzepts • Präsentation des Konzepts an der Vorstandsversammlung der KKJPD • Verabschiedung des Weiterbildungskonzepts durch den Vorstand der KKJPD und Gewährung der Finanzierung • Offizieller Start des Projekts mit Finanzierung • *Request for Information* an vier Unternehmen, mit denen bereits Kontakt aufgenommen wurde	• WTO-konformes *Request for Offer* • Wahl des Anbieters / der Anbieter • Konzeption des E-Learnings
Bedrohungslage	(2) #MISP – Malware Information Sharing Platform vom NCSC für und mit den Kantonen[1]	Marc Barbezat, Leiter Digitale Sicherheit des Kantons Waadt, in Zusammenarbeit mit dem NCSC	• Adoption einer einheitlichen Taxonomie der Cyberbedrohungen durch Bund und Kantone • Kantonaler Cyberbedrohungsradar in Betrieb • Aktiver Austausch von operativen Informationen zu Malware zwischen den Kantonen • Regelmässige Evaluation der Sicherheit ihrer im Internet exponierten peripheren Netzwerkzugangspunkte durch die Kantone • Periodische Veröffentlichung von Berichten zum Monitoring der Cyberbedrohungen	• Ausarbeitung einer einheitlichen Taxonomie der Cyberbedrohungen • Nutzung der Plattform durch 12 Kantone • Schulung von 4 Kantonen durch GovCERT zur Nutzung der Plattform MISP • Begleitung der Kantone bei der aktiven Nutzung der Informationen der Plattform MISP • Erarbeitung eines Ansatzes zur Einrichtung und Weiterentwicklung eines Monitoringprozesses mithilfe von OSINT	• Integration der anderen Kantone in die Plattform MISP • Begleitung der Kantone bei der aktiven Nutzung der Informationen der Plattform MISP • Begleitung der Kantone bei der Einrichtung eines Monitoringprozesses mithilfe von OSINT
Resilienzmanagement	(3) Erhebungstool zur Verbesserung der IKT-Resilienz in den Kantonen	Max Haefeli, Stv. Leiter Informationssicherheit (Deputy CISO) des Kantons Basel-Stadt, in Zusammenarbeit mit dem SVS, dem BWL und der SIK	• Kantone haben anhand des ihnen zur Verfügung gestellten Erhebungstools individuell ihre Defizite in Bezug auf die IKT-Resilienz festgestellt und entsprechende Massnahmen getroffen • Die Durchführung der Erhebung hat dazu geführt, dass gezielte Massnahmen ausgeführt wurden und die IKT-Resilienz sich insgesamt verbessert • Die Resultate der Erhebung wurden in vordefinierten Gremien bspw. Staatsschreiberkonferenz (SSK), Schweizerische Informatikkonferenz (SIK) in anonymisierter Weise vorgestellt	• Erarbeitung und Übersetzung des Erhebungstools • Zustellung des Erhebungstools an alle teilnehmenden Organisationen • Die teilnehmenden Organisationen führen die Erhebung durch • Auswertung von der Projektleitung der erhaltenen Daten • Versand der Auswertung an die teilnehmenden Organisationen • Präsentation der anonymisierten Resultate an der Fachgruppe Cyber des SVS • Austausch mit dem Delegierten des Bundes für Cybersicherheit und dem Geschäftsleiter der SIK	• Präsentation der anonymisierten Resultate an vordefinierten Gremien • Durchführung der Umfrage (ein zweites Mal)

[1] Das Projekt hiess ursprünglich «#MISP – Malware Information Sharing Platform von MELANI für und mit den Kantonen», vgl. Umsetzungsplan, S. 3

	(4) Verstärkter Erfahrungsaustausch über die Schweizerische Informatikkonferenz (SIK) mit der Schaffung von Grundlagen	Arbeitsgruppe Informatiksicherheit der SIK	• Die Kantone stellen sicher, dass der kantonale Informationssicherheitsbeauftragte Mitglied der Arbeitsgruppe „Informatiksicherheit“ der SIK ist • Die Kantone stellen sicher, dass ihre Mitarbeitenden und externen Partner regelmässig bezüglich aller Belange der Informationssicherheit und der Cybersecurity angemessen und stufengerecht geschult und ausgebildet werden • Ein IT-Risikomanagement (Teil des kantonalen Risikomanagements), das auch die Risiken der kritischen Infrastrukturen enthält, ist umgesetzt • Ein der Organisation angepasstes Informationssicherheitsmanagementsystem (ISMS) ist eingeführt	• 17 Kantone entsenden einen Vertreter in die Arbeitsgruppe Informatiksicherheit der SIK • Die Arbeitsgruppe hat vom Umsetzungsplan der Kantone zur NCS und dem Projekt Kenntnis genommen • Mehrere Empfehlungen und Richtlinien wurden von der SIK verabschiedet und den Kantonen zur Verfügung gestellt	
	(5) Sensibilisierung der Bevölkerung für Cyberrisiken	Chantal Billaud, Geschäftsleiterin der Schweizerischen Kriminalprävention (SKP)	• Etablierung und Konsolidierung einer Partnerschaft für die Sensibilisierung der Bevölkerung für Cyberrisiken • Konzeption von zugeschnittenen Lerninhalten	• Die Strukturen, die im Austauschtreffen besprochen werden, wurden geschaffen und die verschiedenen Gruppen (Kerngruppe, Austauschgruppe, Arbeitsgruppen) haben ihre Tätigkeit aufgenommen • Konzeption von Produkten zur Sensibilisierung der Bevölkerung	• Konzeption von weiteren Produkten zur Sensibilisierung der Bevölkerung • Durchführung der Aktionswoche (Social-Media-Kampagne) «Digitale Sicherheit» im Mai 2021
Standardisierung/Regulierung	(6) Umsetzung der Netzwerksicherheitspolicy (NSP)	Arbeitsgruppe Informatiksicherheit SIK, Leitung Adrian Gutknecht in Zusammenarbeit mit dem Kompetenzzentrum Polizeitechnik (PTI)	• Kantonseigene Netzwerk-Sicherheits-Policy wurde erarbeitet und in Anlehnung an die Vorgaben der SIK (NSP-SIK 2017) umgesetzt • Definierte und gelebte Standards • Ausgebildetes Personal • Definierte Prozesse (Change-, Problem-, Incident-, Risiko-, Notfallmanagement sowie Berichtswesen)	• Erarbeitung der Vorgaben für die Umsetzung des Netzwerk-Sicherheitsniveaus anhand der Vorgaben SIK (NSP-SIK 2017) • Erstellen einer Checkliste für die Kantone, zu ihrer Beurteilung des aktuellen Standes ihres Netzwerk-Sicherheitsniveaus (Ist/Soll). • Umsetzung in acht Kantonen sowie im Fürstentum Liechtenstein der (kantons)eigenen NSP anhand der NSP-SIK 2017	• Neun Kantone setzen 2021 ihre kantonseigene NSP um (auf der Basis der NSP-SIK 2017) • Bei weiteren 2 Kantonen erfolgt eine Umsetzung 2022/2023

Krisenmanagement	(7) Cyberübung mit kritischen Infrastrukturen im Gesundheitssektor	Arbeitsgruppe, Leitung André Duvillard, Delegierter des SVS	• Anzahl durchgeführter Übungen mit allen betroffenen Organisationen (1 *Table-Top*-Übung bis 2020, 1 Stabsrahmenübung bis 2021) • Ein aktuelles und präzises Lagebild war während der Übung jederzeit verfügbar und wurde von den teilnehmenden Akteuren adäquat bewertet (Evaluation) • Die an der Übung teilnehmenden Akteure konnten auf die Unterstützung der Stäbe durch fachspezifisches Wissen zählen (Einschätzung der Akteure der Übungserfahrung, Umfrage) • Die Beteiligten kennen die jeweiligen Zuständigkeiten und Ansprechstellen • Die Beteiligten kennen die Prozesse Die Übungen wurden ausgewertet und die Lehren fliessen in die Optimierung der Führungsabläufe und -prozesse ein. Dafür wird ein Monitoringplan aufgesetzt. Die Erkenntnisse werden rapportiert	• Identifikation des USZ als Partner zur Durchführung einer Übung • Durchführung eines Workshops im USZ zur Erarbeitung von Inhalten für das Referenzszenario der Übung	• Erarbeitung des Referenzszenarios für die *Table-Top*-Übung in Zusammenarbeit mit dem NCSC • Fortschritt abhängig von der Verfügbarkeit des USZ vor dem Hintergrund der Covid-19-Pandemie
	(8) Schaffung der kantonalen Organisationen für Cybersicherheit	Arbeitsgruppe, Leitung André Duvillard, Delegierter des SVS	• Richtlinie/Vorlage durch die AG des SVS erarbeitet • In jedem Kanton wurde SOLL/IST-Analyse durchgeführt • Erstellung der kantonalen Cyber-Konzepte: Aufgaben, Kompetenzen und Verantwortung sind in einem kantonalen Cyberkonzept definiert • Die kantonalen Exekutivbehörden haben zur Schaffung der kantonalen Cyberorganisation Beschluss gefasst	• Fertigstellung des Konzepts zur kantonalen Cyberorganisation und Konsultation der verschiedenen Partner (BABS, BA, BWL, KKJPD) • Verabschiedung des Konzepts an der Plenarversammlung der KKJPD im November 2020	• Präsentation des Konzepts an verschiedenen Fachgremien
Aussenwirkung und Sensibilisierung	(9) Aktive Kommunikation zu den Tätigkeiten der Kantone im Rahmen der NCS	André Duvillard, Delegierter des SVS	• Ein Kommunikationskonzept (Leitlinien, Zuständigkeiten, Prozesse) besteht und wurde umgesetzt • Verschiedene Kommunikationsprodukte wurden über diverse Kanäle der interessierten Bevölkerung und den Partnern des SVS zielgruppengerecht und zeitnah zur Verfügung gestellt (Anzahl publizierter Kommunikationsprodukte, Resonanz, Reichweite) • Umfrage zum Bekanntheitsgrad	• Meldungen aus den Kantonen zu ihren Tätigkeiten im Cyberbereich werden auf der Webseite des SVS publiziert • Durchführung der 8. Cyber-Landsgemeinde (August 2020) • Publikation des Jahresberichts zum Stand der Projekte aus dem Umsetzungsplan der Kantone zur NCS	• Organisation und Durchführung der 9. Cyber-Landsgemeinde, die das Ziel verfolgt, über die Fortschritte bei den Projekten des Umsetzungsplans der Kantone zur NCS zu informieren

1. Einleitung

Der Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022 (NCS) wurde von einer Arbeitsgruppe des Sicherheitsverbunds Schweiz (SVS) erarbeitet und am 11. April 2019 von der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) verabschiedet. Strategisches Steuerungsorgan ist die Fachgruppe Cyber des SVS.

Der Umsetzungsplan der Kantone ist integrierender Bestandteil des Umsetzungsplans des Bundes zur NCS und in dessen Anhang zu finden. Zur Gewährleistung einer kohärenten Umsetzung der beiden Pläne (Bund und Kantone) sind der SVS und die KKJPD in der Fachgruppe Cyber des SVS sowie auch im Steuerungsausschuss (StA) NCS vertreten. Der StA NCS, dessen Aufgabe das gemeinsame Projektmanagement ist, stellt die koordinierte, zielgerichtete Umsetzung der NCS-Massnahmen sicher. Zwischen April 2020 und März 2021 ist er zweimal zusammengekommen.

Der Umsetzungsplan der Kantone zur NCS 2018–2022 sieht 13 Projekte in sieben von zehn Handlungsfeldern vor. Vier Massnahmen des Handlungsfelds Strafverfolgung werden von der strategischen Plattform Cyberboard koordiniert, die alle Akteure der Strafverfolgung auf Kantons- und Bundesebene vereinigt. Bei der Mehrheit der anderen neun Projekte ist eine Projektleiterin oder ein Projektleiter aus den Kantonen für die Umsetzung verantwortlich, sie werden dabei vom SVS unterstützt. Die Umsetzung der jeweiligen Projekte basiert auf einem Zeitplan, den die Arbeitsgruppe des SVS an ihrer Sitzung vom 7. Mai 2019 für angemessen erachtete und der gewissen Handlungsspielraum offenlässt.

2. Fachgruppe Cyber des Sicherheitsverbunds Schweiz

Die Fachgruppe Cyber des SVS steht unter dem Vorsitz des Delegierten SVS. In der Fachgruppe vertreten sind die Kantone, das Generalsekretariat der KKJPD, das Generalsekretariat der Konferenz der Kantonsregierungen (KdK), die Schweizerische Kriminalprävention (SKP), die Staatsschreiberkonferenz, die Schweizerische Informatikkonferenz (SIK), der Schweizerische Städteverband, der Schweizerische Gemeindeverband, der Delegierte des Bundes für Cybersicherheit und der Delegierte des VBS für Cyberdefence. Nach der Verabschiedung der NCS 2018–2022 und des Umsetzungsplans der Kantone wurden Auftrag und Zusammensetzung der Fachgruppe Cyber des SVS, die im Zuge der ersten NCS geschaffen wurde, vom Delegierten SVS angepasst. Am 19. August 2019 hat die Politische Plattform des SVS den neuen Auftrag genehmigt. Das Gremium hat sich im Rahmen der zweiten NCS viermal getroffen. Eine seiner Aufgaben besteht in der Koordination der Umsetzung der verschiedenen Projekte aus dem Umsetzungsplan der Kantone. Ausserdem kommt ihm eine wichtige Rolle als Schnittstelle zum StA NCS zu, dem sowohl der Delegierte SVS als auch der Generalsekretär der KKJPD formell angehören.

3. Umsetzungsstand der Projekte

Handlungsfeld 1: Kompetenzen- und Wissensaufbau

Das Projekt **«Entwicklung eines Weiterbildungskonzepts und -moduls für kantonale Verwaltungen»** (Massnahme 2 der NCS «Ausbau und Förderung von Forschungs- und Bildungskompetenz») sieht die Ausgestaltung eines umfassenden Weiterbildungsprogramms für das Verwaltungspersonal vor. Bei der Umsetzung des Projekts wurden einige bedeutende Fortschritte erzielt. Nachdem eine partielle Bestandsaufnahme der in den Kantonen vorhandenen Weiterbildungen vorgenommen worden war und eine dedizierte Arbeitsgruppe ein Weiterbildungskonzept erstellt hatte, genehmigte der Vorstand der KKJPD das Konzept und gewährte 2020 das für die Konzeption erforderliche Budget. Die Arbeitsgruppe sowie die Unterarbeitsgruppen, die sich aus Informationssicherheitsbeauftragten von Bund und Kantonen zusammensetzen, befassten sich mit der Ausarbeitung einer didaktischen Matrix, der Festlegung von Begleitmassnahmen und der Klärung der Anforderungen an die IT-

Umgebungen der Kantone. Ferner wurde vier Unternehmen, mit denen bereits Kontakt aufgenommen worden war, ein *Request for Information* vorgelegt. Eine WTO-konforme Ausschreibung befindet sich in Vorbereitung. Das Weiterbildungsprogramm wird sich an das gesamte Personal der Kantons- und Gemeindeverwaltungen richten. Diskutiert wird zudem, ob auch die Mitarbeitenden verschiedener Departemente der Bundesverwaltung von dieser Weiterbildung profitieren können. Die Umsetzung entsprechender Weisungen und Empfehlungen in den Kantonen variiert allerdings und hängt in erster Linie von den Ressourcen ab, die im Bereich der Informationssicherheit im jeweiligen Kanton vorhanden sind.

Handlungsfeld 2: Bedrohungslage

Im Rahmen des Projekts **«#MISP – Malware Information Sharing Platform»**, das zur Umsetzung der Massnahme 4 der NCS «Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyberbedrohungslage» beiträgt, erarbeitete das Nationale Zentrum für Cybersicherheit (NCSC) auf der Grundlage der Cybercrime-Phänomeneblätter von fedpol eine Referenztaxonomie für Cyberbedrohungen. Diese Taxonomie wurde zur Verwendung in den Verwaltungen erstellt, damit diese über eine gemeinsame Sprache verfügen. Sie wurde an der vom SVS am 27. August 2020 organisierten Cyber-Landsgemeinde vorgestellt und war Gegenstand eines eigenen Workshops. Die Plattform MISP wird von zwölf Kantonen (AG, BS, GE, GR, JU, LU, SZ, SO, VD, VS, ZH, ZG) als Informationsquelle genutzt, wodurch diese Kantone ihre Fähigkeit verbessern, Cyberrisiken zu definieren und zu analysieren. 2020 führte GovCERT insgesamt drei Schulungen zur Nutzung der Plattform MISP durch. Daran nahmen rund 130 Personen teil, darunter sechs kantonale Teilnehmerinnen und Teilnehmer aus vier verschiedenen Kantonen. Die Lage rund um die Covid-19-Pandemie hat sich merklich auf die Umsetzung dieses Projekts ausgewirkt. So ist es beispielsweise nicht einfach, unter Sicherstellung der Vertraulichkeit Online-Workshops für ein grosses Publikum zu organisieren.

Handlungsfeld 3: Resilienzmanagement

Das Projekt **«Erhebungstool zur Verbesserung der IKT-Resilienz in den Kantonen»** (Massnahme 5 der NCS «Verbesserung der IKT-Resilienz der kritischen Infrastrukturen») sieht vor, dass die Kantone die erforderlichen minimalen Anforderungen in Bezug auf Prozesse, Kompetenzen und Aufgaben analysieren. Diese Analyse erfolgt mithilfe eines Erhebungstools, das von Max Haefeli, dem Stv. Leiter Informationssicherheit (Deputy CISO) des Kantons Basel-Stadt, erarbeitet wurde und auf dem Analyse-Tool «Minimalstandard zur Verbesserung der IKT-Resilienz» des Bundesamts für wirtschaftliche Landesversorgung (BWL) basiert. Die an diesem Projekt teilnehmenden Organisationen, mehrheitlich Kantone, haben die Analyse 2020 durchgeführt. Nachdem die Daten von der Projektleitung ausgewertet worden waren, erhielten die teilnehmenden Organisationen ihre anonymisierten Resultate im Vergleich zu jenen der anderen Organisationen. Dies ermöglichte ihnen, ihre Defizite in Bezug auf die IKT-Resilienz festzustellen und zu beurteilen. Darauf basierend können sie nun gezielte Sicherheitsmassnahmen zur Risikominderung und zur Stärkung ihrer Sicherheitsorganisation ergreifen. Die Resultate wurden überdies in der Fachgruppe Cyber des SVS präsentiert und mit dem Delegierten des Bundes für Cybersicherheit besprochen. Es ist vorgesehen, dass sie im Laufe der Zeit in ausgewählten Gremien vorgestellt werden und dass die Erhebung ein weiteres Mal durchgeführt wird.

Im Rahmen des Projekts «**Verstärkter Erfahrungsaustausch über die Schweizerische Informatikkonferenz (SIK) mit der Schaffung von Grundlagen**» (Umsetzung von Massnahme 7 der NCS «Erfahrungsaustausch und Schaffung von Grundlagen zur Stärkung der IKT-Resilienz in den Kantonen») fördern die Kantone ihre Zusammenarbeit durch die Institutionalisierung des Erfahrungsaustauschs und des Dialogs, um dadurch ihre IKT-Resilienz zu verbessern. Zu diesem Zweck greifen die Kantone auf bestehende Netzwerke zurück: etwa auf die SIK und ihre Arbeitsgruppe Informations- und Cyber-Sicherheit, die für die

Umsetzung des Projekts verantwortlich ist und in der 17 Kantone sowie andere Organisationen (das Bundesamt für Informatik und Telekommunikation BIT, das Eidgenössische Finanzdepartement EFD mit dem NCSC, u.a.) vertreten sind. Ziel der Arbeitsgruppe ist es, Empfehlungen oder Richtlinien zu aktuellen Themen der Informationssicherheit zu verfassen und den Mitgliedern der SIK zur Verfügung zu stellen. Die SIK hat kürzlich auf ihrem Intranet einen Bericht veröffentlicht, in dem die Voraussetzungen für die einfache Anwendung von sicheren und benutzerfreundlichen Lösungen für Videokonferenzen zwischen öffentlichen Verwaltungen definiert werden. Das Thema sichere Online-Konferenzlösungen wird von der neu gegründeten SIK-Arbeitsgruppe Cloud Governance weitergeführt. Diese Arbeitsgruppe behandelt rechtliche und technische Fragen zum Cloud-Einsatz in der öffentlichen Verwaltung und ist für Sicherheitsfragen in engem Austausch mit der AG Informations- und Cyber-Sicherheit. Des Weiteren hat die SIK eine Empfehlung zum Thema «Monitoring von Security-Anomalien» ausgearbeitet, die an der ersten Sitzung der Arbeitsgruppe 2021 verabschiedet und allen Kantonen zur Verfügung gestellt wurde. Zudem verabschieden die Kantone voraussichtlich noch 2021 die Richtlinie mit den definierten Vorgaben zum IKT Grundschutz.

Die im Rahmen des Projekts **«Sensibilisierung der Bevölkerung für Cyberrisiken»**[2] vorgesehenen Aktivitäten zielen darauf ab, durch die Verstärkung der allgemeinen Prävention in der Bevölkerung die Resilienz der Schweiz in Bezug auf Cyberrisiken zu verbessern. Trotz der Situation rund um die Covid-19-Pandemie wurde die Zusammenarbeit zwischen dem Netzwerk Ermittlungsunterstützung Digitale Kriminalitätsbekämpfung (NEDIK) und den für die Projektumsetzung geschaffenen Arbeitsgruppen im Jahr 2020 weitergeführt. Die Schweizerische Kriminalprävention (SKP) veröffentlichte im Berichtszeitraum zahlreiche Produkte zur Sensibilisierung der Bevölkerung, die verschiedene Themenbereiche abdecken. Nachfolgend sind einige Beispiele aufgeführt:

- «My little little Safebook» und «Dein Leben online»: zwei Faltblätter, die sich an Jugendliche und Erziehungsberechtigte richten und darüber informieren, wie man sich im Internet und im Falle von Cybermobbing verhalten soll;
- Drei Präventionsclips zu den Themen *Sextorsion*, betrügerische Supportanrufe und *Cybergrooming*;
- Mitherausgabe des zweiten Comicbands des Bundesamts für Kommunikation (BAKOM), «Geschichten aus dem digitalen Alltag», der Themen wie Fake News, *Sexting*, Mobbing, Datenschutz und Abhängigkeit vom Smartphone aufgreift;
- das Faltblatt «5 Schritte für Ihre digitale Sicherheit», das in Zusammenarbeit mit «eBanking – aber sicher!» (EBAS) entstand und erklärt, welche Grundsätze es zu befolgen gilt, um sich und die eigene IT-Infrastruktur vor Cyberkriminellen zu schützen;
- die schweizweite Kampagne «Card Security gegen Kartendelikte» der Stadtpolizei Zürich (siehe https://www.card-security.ch/de/home).

Sämtliche Druck- und Onlineprodukte, die von der SKP oder einem Polizeikorps realisiert und von der SKP übersetzt und vertrieben wurden, wurden über die Kommunikationskanäle aller Polizeikorps weit verbreitet. Auch von der Bevölkerung wurden sie breit aufgegriffen und über die sozialen Netzwerke und Medien weiterverbreitet. Für 2021 sind weitere Produkte zur Sensibilisierung der Bevölkerung geplant. Was die Zusammenarbeit mit den relevanten Akteuren angeht, so tauscht sich die SKP regelmässig mit der Kantonspolizei Zürich über die neuen Cybercrime-Phänomene aus. Letztere hat im November 2019 die Website www.cybercrimepolice.ch lanciert, welche die Bevölkerung für Cyberkriminalität sensibilisieren soll. Die Zusammenarbeit mit dem NCSC, iBarry und EBAS hat sich 2020 intensiviert, bedingt durch die Vorbereitungen für die Aktionswoche (Social-Media-Kampagne) «Digitale Sicherheit», die im Mai 2021 stattfinden soll.

[2] Das Projekt hiess ursprünglich «Sensibilisierung der jungen und älteren Menschen für Cyberrisiken», vgl. Umsetzungsplan, S. 7

Handlungsfeld 4: Standardisierung/Regulierung

Die Kantone sehen im Rahmen der Massnahme 8 der NCS 2018-22 «Entwicklung und Einführung von Minimalstandards» vor, die **von der SIK 2017 erarbeitete Netzwerksicherheitspolicy** (für alle Mitglieder auf dem Intranet zugänglich) umzusetzen. 2018 wurden Vorgaben für die Umsetzung der Netzwerksicherheitspolicy in den Kantonen erarbeitet und von der SIK verabschiedet. Anschliessend erstellte die Arbeitsgruppe eine Checkliste für die Beurteilung des Umsetzungsgrads hinsichtlich der Netzwerksicherheitspolicy der SIK, die den Kantonen zugestellt wurde, damit diese das erforderliche Referenzniveau ermitteln können. Bis heute haben acht Kantone sowie Liechtenstein eine (kantons)eigene Netzwerksicherheitspolicy (in Anlehnung an jene der SIK) umgesetzt. Elf weitere Kantone planen die Umsetzung bis 2023. Auf dieser gemeinsamen Grundlage betreiben die Kantone ihre Netzwerke und Systeme und stellen gleichzeitig eine laufende Überwachung der Aktivitäten innerhalb ihres eigenen Netzwerks sicher und erhöhen so ihre Sicherheit. Die Umsetzung der Netzwerksicherheitspolicy ist allerdings abhängig von langfristigen Prozessen, etwa technischen und architektonischen Anpassungen an den Netzwerkinfrastrukturen oder Budgetplanungen.

Handlungsfeld 5: Krisenmanagement

Im Rahmen des Projekts **«Cyberübung mit kritischen Infrastrukturen im Gesundheitssektor»** (Massnahme 17 der NCS «Gemeinsame Übungen zum Krisenmanagement») soll zuerst eine *Table-Top*-Übung mit Cyberausprägung in einer kritischen Infrastruktur im Gesundheitssektor sowie anschliessend eine Stabsrahmenübung durchgeführt werden. Bei der Umsetzung, für die der SVS verantwortlich zeichnet, gab es aufgrund der Covid-19-Pandemie eine Änderung im Zeitplan. Das Universitätsspital Zürich (USZ), das vom SVS für die Umsetzung als Partner gewonnen werden konnte, war stark in die Pandemiebewältigung involviert. Trotz der schwierigen Situation tauschten sich der SVS und das USZ regelmässig aus, was schliesslich in der Organisation eines Workshops resultierte. Unterstützt durch das NCSC und Markus Meile, Stabschef der Städtischen Führungsorganisation der Stadt Zürich, brachte der Workshop, der im Herbst 2020 stattfand, den SVS und die für ausserordentliche Lagen zuständige Fachgruppe des USZ zusammen. Ziel des Workshops war es, das Arbeitsumfeld der Mitarbeitenden des USZ besser zu verstehen und für die Ausarbeitung des Referenzszenarios einige grundlegende Informationen zusammenzutragen. Gegenwärtig arbeitet der SVS zusammen mit dem NCSC am Referenzszenario für die *Table-Top*-Übung und hofft, die Übung im Laufe des Jahres 2021 durchführen zu können. Die Fortschritte bei der Umsetzung hängen allerdings von der Verfügbarkeit des USZ angesichts der Covid-19-Pandemie ab.

Bei der Umsetzung des Projekts **«Schaffung der kantonalen Organisationen für Cybersicherheit»** hat der SVS wichtige Meilensteine erreicht. Die Arbeitsgruppe des SVS, die vom Delegierten SVS geleitet wird und aus Vertretungen der Kantone Basel-Stadt, Freiburg, Genf, Tessin, Zürich sowie vom Fürstentum Liechtenstein und vom Nationalen Zentrum für Cybersicherheit besteht, hat nach Konsultation der verschiedenen Partner (BABS, BA, BWL, KKJPD) das Konzept «Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation» ausgearbeitet und fertiggestellt. Im November 2020 wurde das Konzept an der Plenarversammlung der KKJPD verabschiedet. Im Laufe des Jahres 2021 wird es verschiedenen Fachgremien vorgestellt. Die darin enthaltenen Empfehlungen, die den Kantonen zur Verfügung stehen, werden die Arbeiten der zuständigen Behörden bei der Schaffung einer kantonalen Cyberorganisation vereinfachen.

Handlungsfeld 6: Aussenwirkung und Sensibilisierung

Der SVS trägt auch im Interesse der Kantone dazu bei, ihre Arbeiten im Rahmen der NCS sichtbar zu machen. Im Rahmen des Projekts **«Aktive Kommunikation zu den Tätigkeiten**

der Kantone im Rahmen der NCS» (Massnahme 28 der NCS «Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS») werden die Tätigkeiten der Kantone auf dem Gebiet der Cybersicherheit regelmässig auf der Website des SVS publiziert (svs.admin.ch). Ferner hat der SVS im August 2020 die 8. Cyber-Landsgemeinde organisiert, die neben dem Austausch unter den betreffenden Akteuren das Ziel verfolgt, über die Fortschritte bei den Projekten des Umsetzungsplans der Kantone zur NCS zu informieren. Zu diesem jährlichen Anlass fanden sich über 100 Teilnehmende vor allem aus den Kantonen und des Bundes ein.

4. Entwicklung der Cyberstrukturen des Bundes und Einbindung der Kantone

Die Umsetzung und Entwicklung der Strukturen des Bundes im Bereich Cybersicherheit, wie sie der Bundesrat im Januar 2019 verabschiedet hat, wurde 2020 fortgesetzt.

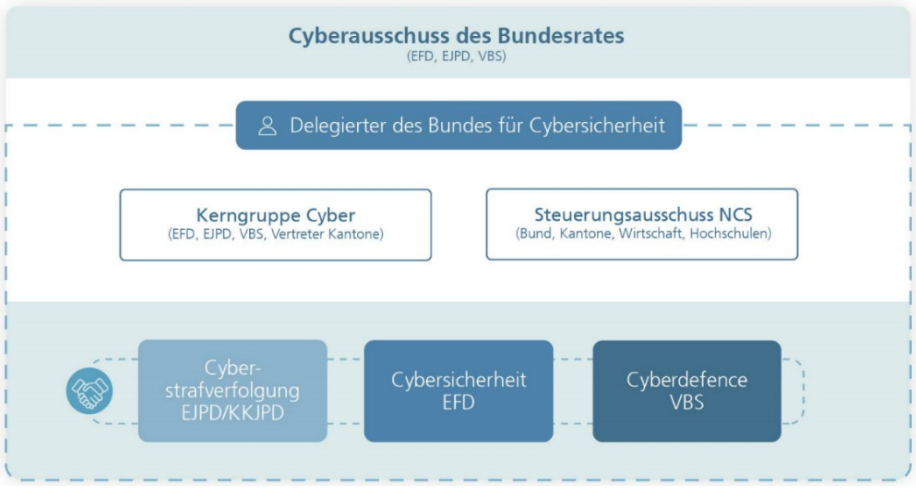

Abbildung I: Organisation des Bundes im Bereich Cybersicherheit (Quelle: NCSC)

Die Kantone sind in allen drei Koordinationsgremien vertreten. Der Präsident der KKJPD nimmt an den Sitzungen des Cyberausschusses des Bundesrats teil, der Präsident der KKPKS an jenen der Kerngruppe Cyber und im StA NCS sind die Kantone über das Generalsekretariat der KKJPD und den Delegierten SVS vertreten.

Der Delegierte des Bundes für Cybersicherheit, der seit August 2019 in dieser Funktion tätig ist, hat unter anderem die Aufgabe, zum Schutz der Schweiz vor Cyberrisiken eine optimale Koordination der Arbeiten der Kantone und des Bundes sicherzustellen. Im Rahmen der Umsetzung der NCS wurden die Kantone folglich in die Aktivitäten des Delegierten eingebunden. In den vergangenen zwölf Monaten hat sich der Austausch zwischen dem Delegierten des Bundes für Cybersicherheit und dem SVS intensiviert, sodass sich eine echte Partnerschaft zwischen den beiden Parteien entwickelt hat.

An seiner Sitzung vom 27. Mai 2020 verabschiedete der Bundesrat die Cyberrisikenverordnung, welche die rechtliche Grundlage für den Aufbau des Nationalen Zentrums für Cybersicherheit (NCSC) schafft. Gleichzeitig beschloss er für die Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2020–2022, die personellen Ressourcen um 20 Stellen zu verstärken. In das unter der Leitung des Delegierten des Bundes für Cybersicherheit stehende NCSC eingegliedert sind fortan die Fachstelle für die Informatiksicherheit des Bundes, die Melde- und Analysestelle Informationssicherung (MELANI) sowie das nationale Computer Emergency Response Team (GovCERT) als Fachstelle. Seit dem 21. Dezember 2020 ist, bereitgestellt durch das NCSC, ein neues nutzergeführtes Meldeformular für freiwillige Meldungen von Cybervorfällen verfügbar, bei dem die Benutzerfreundlichkeit und der direkte Mehrwert für Meldende im Mittelpunkt steht. Zur gleichen Zeit ging die überarbeitete Website des NCSC online.

Die Absicht des NCSC ist es, die Kantone, Hochschulen und Wirtschaftskreise, die über spezifische Kompetenzen verfügen, in sein Netzwerk einzubinden. Vor diesem Hintergrund besteht zwischen dem SVS und dem NCSC eine Zusammenarbeit bei der Umsetzung des Mandats bezüglich eines Kompetenznetzwerks Cybersicherheit, das die Politische Plattform des SVS im März 2020 erteilt hat. Der SVS wurde damit beauftragt, in den Kantonen eine Bestandsaufnahme der Kompetenzen und Leistungen im Bereich der Cybersicherheit durchzuführen und die Grundlage für eine strukturierte Zusammenarbeit zwischen dem NCSC und den Kantonen zu schaffen. Aus den Ergebnissen geht hervor, dass in den Kantonen erst wenige Kompetenzen und Leistungen vorhanden sind, die auf regionaler oder gar nationaler Ebene angeboten werden könnten. Eine in einem zweiten Schritt bei den Hochschulen durchgeführte Umfrage ergab jedoch, dass an den Fachhochschulen mehrere Projekte und Angebote für KMU bestehen. Schliesslich zeigte die Umfrage auch, dass im Bereich der Cybersicherheit eine breite Palette an Weiterbildungsangeboten (CAS, MAS, DAS usw.) existiert. Diese werden künftig in Form einer Liste der Öffentlichkeit zugänglich gemacht.

5. Weitere Aktivitäten der Geschäftsstelle des Delegierten SVS

Im Kampf gegen die Cyberkriminalität arbeiten die Kantone mit den Strafverfolgungsbehörden auf Bundesebene zusammen. Dabei werden sie in der strategischen Plattform des Cyberboards, die 2018 geschaffen wurde, vom Delegierten SVS vertreten. Dies ermöglicht eine verstärkte Koordination bei der gemeinsamen Bearbeitung von interkantonalen und internationalen Fällen. Zudem ist der Delegierte SVS Mitglied der VBS Expert Group. Damit verfügt er über einen Gesamtüberblick über die Herausforderungen in den Bereichen Cybersicherheit, Cyberabwehr und Cyberkriminalität.

Des Weiteren verfasste der SVS in Zusammenarbeit mit der Kantonspolizei Bern in der Zeitschrift «Schweizer Gemeinde» des Schweizerischen Gemeindeverbands (Ausgabe Mai 2020) einen Artikel zum Umgang mit Cyberrisiken in den Gemeinden.

6. Bilanz und Ausblick

Der Berichtszeitraum war durch die Situation im Zusammenhang mit der Covid-19-Pandemie geprägt, die sich deutlich auf den Fortschritt der Arbeiten auswirkte. Die Umsetzung der Projekte, die im Umsetzungsplan der Kantone zur NCS vorgesehen sind, wurde in erster Linie durch diese beispiellose Situation belastet – aber auch durch die bereits existierenden Herausforderungen im Zusammenhang mit den unterschiedlichen bestehenden Strukturen, Ressourcen und Personalbeständen in den Kantonen.

Trotz dieser Hindernisse ist klar erkennbar, dass bei der Umsetzung einiger Projekte wichtige Meilensteine erreicht wurden. Dies ist dem Engagement der Projektverantwortlichen zu verdanken, die mehrheitlich aus den kantonalen Strukturen kommen und ihre Arbeiten ungeachtet der Turbulenzen voranzutreiben versuchten. Die Kantone haben somit den Schutz ihrer Verwaltung und der Bevölkerung vor Cyberrisiken verstärkt. Die Bemühungen der Kantone im Bereich der Cybersicherheit resultierten beispielsweise in der Verabschiedung der ersten kantonalen Strategie zum Schutz vor Cyberrisiken durch die Kantonsregierung St. Gallen.

2021 sind die verschiedenen Projekte gemäss Zeitplan soweit möglich voranzutreiben, wobei deren Umsetzung unter anderem von der weiteren Entwicklung der Situation rund um die Covid-19-Pandemie abhängt. Auch sind im Rahmen der ersten Reflexionen zur Ausarbeitung der dritten NCS, zu denen in Kürze der Startschuss fällt, die Interessen und Bedürfnisse der Kantone zu berücksichtigen, zumal die Kantone zentrale Akteure im Bereich der Cybersicherheit sind.