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 2022

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 2021 bis März 2022) 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 • Ausschreibung (WTO-konform),Wahl des Anbieters und Vertragsabschluss • Planung und Beginn der Realisierung • Hinzufügen eines neuen Icons «Behörden» auf der Website ncsc.ch (Begleitmassnahme)	• 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 14 Kantone • Schulung von 4 Kantonen durch das NCSC 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	• Organisation durch das NCSC von Schulungen zur Nutzung der Plattform MISP • Selbstevaluation der Kantone bezüglich ihrer Abwehrbereitschaft gegenüber Cyberbedrohungen durch Ransomware
Resilienzmanagement	(3) Erhebungstool zur Verbesserung der IKT-Resilienz in den Kantonen	Sicherheitsverbund Schweiz SVS in Zusammenarbeit mit Max Haefeli, (neu : Haefeli Consulting)	• 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	• Erarbeitung und Übersetzung des Erhebungstools • Zustellung des 1. Erhebungstools an alle teilnehmenden Organisationen • Die teilnehmenden Organisationen führen die 1. Erhebung durch • 1. Auswertung von der Projektleitung der erhaltenen Daten	• Auswertung der Resultate der zweiten Erhebung

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

			• Die Resultate der Erhebung wurden in vordefinierten Gremien, bspw. Staatsschreiberkonferenz (SSK), Schweizerische Informatikkonferenz (SIK), in anonymisierter Weise vorgestellt	• Versand der 1. Auswertung an die teilnehmenden Organisationen • Präsentation der anonymisierten Resultate in der Fachgruppe Cyber des SVS • Austausch mit dem Delegierten des Bundes für Cybersicherheit und dem Geschäftsleiter der SIK • Präsentation der anonymisierten Resultate in vordefinierten Gremien • Vorbereitung der 2. Erhebung	
	(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 • Im Rahmen der 9. Cyber-Landsgemeinde fanden ein Austausch mit den Mitgliedern und ein Workshop über die Auswirkungen des «Solarwind Hacks» statt • Per 1. Januar 2022 wurden die Aktivitäten der SIK an die Digitale Verwaltung Schweiz (DVS) übertragen	
	(5) Sensibilisierung der Bevölkerung für Cyberrisiken[2]	Fabian Ilg, Geschäftsleiter 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 • Online-Sensibilisierungskampagne in Zusammenarbeit mit dem NCSC, iBarry und «E-Banking – aber sicher!» (EBAS)	• Konzeption von weiteren Produkten zur Sensibilisierung der Bevölkerung • Fortsetzung der Zusammenarbeit mit den einschlägigen Akteuren und Stärkung der bereits bestehenden Partnerschaften
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	• Elf Kantone setzen ihre kantonseigene NSP bis 2023 um (auf der Basis der NSP-SIK 2017) • Fortsetzung der Umsetzung voraussichtlich über die Laufzeit der NCS 2018–2022 hinaus

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

				aktuellen Standes ihres Netzwerk-Sicherheitsniveaus (Ist/Soll) • Umsetzung in acht Kantonen sowie im Fürstentum Liechtenstein der (kantons)eigenen NSP anhand der NSP-SIK 2017 • Informieren der Kantone über das neue Informationssicherheitsgesetz und Austausch darüber	
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 • Vorbereitung der Übung, Entwicklung der Methode, der Ziele und des Referenzszenarios • Organisation einer *Table-Top*-Übung durch den SVS im Dezember 2021	• Organisation einer Stabsrahmenübung
	(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 zur kantonalen Cyberorganisation an verschiedenen Fachtagungen • Laufende / geplante Umsetzung der Empfehlungen entsprechend dem Konzept in mehreren Kantonen (u. a. LU, ZH, BS, VD, SG, AG)	• Aktualisierung des Konzepts zur kantonalen Cyberorganisation
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 Website des SVS publiziert • Durchführung der 9. Cyber-Landsgemeinde (September 2021) • Publikation des Jahresberichts zum Stand der Projekte aus dem Umsetzungsplan der Kantone zur NCS	• Organisation und Durchführung der 10. 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.

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 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 wurde der Auftrag der Fachgruppe Cyber des SVS, die im Zuge der ersten NCS geschaffen worden war, vom Delegierten SVS angepasst. Am 19. August 2019 hat die Politische Plattform SVS den neuen Auftrag genehmigt. Ebenfalls überprüft wurde die Zusammensetzung der Fachgruppe. Zu deren Mitgliedern gehört seit Kurzem Peppino Giarritta, der Beauftragte von Bund und Kantonen für die Digitale Verwaltung Schweiz (DVS). Die neue Organisation DVS, die strukturell dem SVS ähnlich ist, wurde am 1. Januar 2022 vom Bundesrat und den Kantonsregierungen gegründet, um die Zusammenarbeit zwischen Bund, Kantonen, Gemeinden und Städten bei der Umsetzung und Steuerung der digitalen Transformation der Verwaltung zu stärken. Die Einbindung des neuen Beauftragten DVS in die Fachgruppe Cyber des SVS ist ein erster Schritt in Richtung einer intensiveren Zusammenarbeit zwischen dem SVS und der DVS beziehungsweise einer weiteren Annäherung der Bereiche Cybersicherheit und digitale Transformation.

Die Aufgaben der Fachgruppe Cyber des SVS bestehen in erster Linie in der Koordination der Umsetzung der verschiedenen Projekte aus dem Umsetzungsplan der Kantone. Ausserdem kommt ihr eine wichtige Rolle als Schnittstelle zum StA NCS zu, dem sowohl der Delegierte SVS als auch ein Mitglied des Generalsekretariats 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 Personal der Verwaltungen von Bund, Kantonen und Gemeinden vor. Nachdem eine dedizierte Arbeitsgruppe eine partielle Bestandsaufnahme der in den Kantonen vorhandenen Weiterbildungen vorgenommen und ein Weiterbildungskonzept erstellt hatte, genehmigte der Vorstand der KKJPD das Konzept und gewährte das für die Konzeption erforderliche Budget. Auf den *Request for Information* antworteten vier Unternehmen, mit denen bereits Kontakt aufgenommen worden war. Daraufhin führte die Arbeitsgruppe eine WTO-konforme Ausschreibung durch und wählte schliesslich den Anbieter. Ferner wurden die Arbeiten zur Konzeption des E-Learnings geplant und die Realisierung hat begonnen.

Zudem wurde eine von der Arbeitsgruppe definierte Begleitmassnahme umgesetzt, die darin besteht, auf der Website des Nationalen Zentrums für Cybersicherheit (ncsc.ch) unter einem neuen Icon «Behörden» den Behörden die nötigen Informationen zu aktuellen Bedrohungen und dem Vorgehen im Falle eines Cyberangriffs bereitzustellen.

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 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. Was das Hauptziel dieses Handlungsfelds angeht, so wird die Plattform MISP von MELANI von 14 Kantonen (AG, BS, GE, GR, JU, LU, SZ, SO, VD, VS, ZH, ZG sowie BE und SG über ihre Service-Provider) als Informationsquelle genutzt, wodurch diese Kantone ihre Fähigkeit verbessern, Cyberrisiken zu definieren und zu analysieren. Ferner führte das NCSC 2021 im Rahmen dieses Projekts zehn Schulungen mit durchschnittlich rund 20 Teilnehmerinnen und Teilnehmern durch. Dabei ist die Durchführung als Online-Workshop bei diesem Projekt zur Norm geworden. Die Schulungen werden 2022 weitergeführt und durch eine Umfrage ergänzt, in deren Rahmen die Kantone ihre Abwehrbereitschaft gegenüber Cyberangriffen mithilfe einer Selbstevaluation beurteilen.

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. Die Durchführung der Erhebung ist in der Strategieperiode 2018–2022 zweimal vorgesehen, womit die zentralen Aktivitäten im Rahmen dieser Massnahmen im vergangenen Jahr vor allem mit der Vorbereitung der zweiten Erhebung im Zusammenhang standen. Die Analyse wird durch ein Erhebungstool im Excel ermöglicht, das von Max Haefeli, mittlerweile Inhaber von «Haefeli Consulting», auf Basis des IKT-Minimalstandards[3] konzipiert und auf die Bedürfnisse der Kantone angepasst wurde. Der Versand aller Dokumente und Hilfsmittel zur zweiten Erhebungsrunde erfolgte im Dezember 2021, die Frist zum Einreichen der ausgefüllten Formulare läuft bis Ende März 2022. Die wiederholte Teilnahme an der schweizweiten Erhebung erlaubt es den Kantonen eine Momentaufnahme über die IKT-Resilienz ihrer Organisation zu machen, aber vor allem den anonymen Vergleich unter Gleichartigen. Besonders interessant ist ausserdem, dass die einzelnen Kantone ihren Fortschritt im Vergleich visualisieren können.

[3] «Minimalstandard zur Verbesserung der IKT-Resilienz» des Bundesamts für wirtschaftliche Landesversorgung (BWL)

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.

Die SIK-Arbeitsgruppe Cyber- und Informationssicherheit unter dem Vorsitz von A. Gutknecht tagte in der Berichtsperiode weiterhin regelmässig. Im ersten Halbjahr konnte sie zwei Empfehlungen verabschieden. Dabei handelt es sich erstens um eine Empfehlung zur Veröffentlichung von Informationen über ICT-Personal. Eine zweite Empfehlung thematisierte den Aufbau eines Security Monitorings (mit oder ohne Security Operations Center (SOC)). Auch Guidelines als Empfehlung zum Umgang mit IoT von der SIK-Arbeitsgruppe Telekom gehen auf diese Berichtsperiode zurück.

Die Gründung der Arbeitsgruppe Cloud Governance geht bereits auf September 2020 zurück. Sie erarbeitet Grundlagen, Hilfsmittel und Best-Practice-Ansätze für die Integration und Nutzung von Cloud-Diensten in der öffentlichen Verwaltung. Die Arbeitsgruppe setzt sich aus über 20 Mitarbeitenden von Bund, Kantonen und Städten zusammen. Die Arbeitsgruppe hat im Austausch mit diversen Partnern den Bereich Datenschutz besonders intensiv analysiert und im Sinne der Rechtssicherheit Standardklauseln für die Ausgestaltung von Verträgen mit ICT-Dienstleistern formuliert. Die Bereitstellung von Musterverträgen sowie die Aushandlung von Vertragsbedingungen ist ein zentrales Angebot der SIK, weil die Bündelung von Anforderungen und Volumina bei der Verhandlung mit Anbietern von ICT-Dienstleistungen Vorteile bringt.

Zur Verbesserung der Cybersicherheit in den Gemeinden hat die SIK zusammen mit der Forschungsstelle der ETH Zürich rund um das Produkt SCION (Internet für den sicheren Datentransfer) eine Machbarkeitsstudie initiiert.

Besondere Erwähnung gilt abschliessend den Auswirkungen des «Solarwind Hack» auf die öffentlichen Verwaltungen, der die Security-Verantwortlichen monatelang beschäftigt hat. Die SIK hat die Bedrohungslage im Dezember 2020 im Austausch mit ihren Mitgliedern erörtert und veranstaltete im Rahmen der Cyber-Landsgemeinde im August 2021 einen Workshop mit Interessierten der Kantone und des Bundes, um vertiefte Expertisen und Erfahrungen auszutauschen.

Die Tätigkeiten der SIK gingen per 1. Januar 2022 an die Digitale Verwaltung Schweiz (DVS) über.

Die im Rahmen des Projekts «**Sensibilisierung der Bevölkerung für Cyberrisiken**» vorgesehenen Aktivitäten zielen darauf ab, durch die Verstärkung der allgemeinen Prävention in der Bevölkerung die Resilienz der Schweiz in Bezug auf Cyberrisiken zu verbessern. In diesem Zusammenhang hat die Schweizerische Kriminalprävention (SKP) eine starke Partnerschaft mit dem Netzwerk Ermittlungsunterstützung Digitale Kriminalitätsbekämpfung (NEDIK) und cybercrimepolice.ch aufgebaut und tauscht sich zudem regelmässig mit dem NCSC über die Sensibilisierung und Cybercrime-Phänomene aus. Mehrere Produkte zur Sensibilisierung gegenüber Cyberrisiken wurden konzipiert, der Bevölkerung zur Verfügung gestellt und über die verschiedenen Kommunikationskanäle der SKP verbreitet. Die SKP hat überdies ihre Präsenz in verschiedenen sozialen Netzwerken verstärkt und ausgebaut, um ihre Sichtbarkeit im Netz zu erhöhen. Im Berichtszeitraum hat sie die folgenden Projekte umgesetzt:

- die Online-Sensibilisierungskampagne «S-U-P-E-R», die auf die fünf Schritte für die digitale Sicherheit fokussiert und in Zusammenarbeit mit dem NCSC, EBAS und iBarry entstand;
- das Faltblatt «Rendite genial? Verlust total!» sowie die Sensibilisierung mehrerer Finanzinstitute mithilfe der Schweizerischen Bankiervereinigung, dem Schweizerischen Versicherungsverband und dem Schweizerischen Pensionskassenverband;
- drei neue Präventionsclips zu den Themen *Sexting*, Immobilienbetrug und Anlagebetrug;
- die Koordinierung und Verbreitung der Kampagne #ufpasse der Zürcher Stadtpolizei, die im Rahmen von Card Security lanciert wurde und die Bevölkerung auf die Risiken beim Onlineshopping mit Debit- und Kreditkarten aufmerksam machen soll.
  Diese Massnahme richtet sich an die gesamte Bevölkerung. Im Rahmen derSensibilisierungsarbeit zum Thema Anlagebetrug wurden jedoch Anstrengungen unternommen, die Bevölkerungsgruppe der über 50-Jährigen anzusprechen, indem mit Institutionen, die Weiterbildungen für die Ruhestandsplanung anbieten (zum Beispiel Publica), Kontakt aufgenommen wurde.

Handlungsfeld 4: Standardisierung/Regulierung

Die Kantone sehen im Rahmen der Massnahme 8 der NCS 2018–2022 **«Entwicklung und Einführung von Minimalstandards»** vor, die von der SIK 2017 erarbeitete Netzwerksicherheitspolicy NSP-2017 (für alle Mitglieder auf dem Intranet der SIK zugänglich) umzusetzen. Der Umsetzungsstand entspricht grösstenteils demjenigen aus der letzten Berichtsperiode. Es haben weiterhin acht Kantone sowie Liechtenstein eine (kantons)eigene Netzwerksicherheitspolicy (NSP) (in Anlehnung an jene der SIK) umgesetzt. Elf weitere Kantone planen die Umsetzung bis 2023. Es ist absehbar, dass die Umsetzung der NSP-2017 in den verbleibenden Kantonen noch über die Strategieperiode andauern wird. Nichtsdestotrotz war der geforderte Minimalstandard in den Kantonen auch im vergangenen Jahr ein wichtiges Thema. So hat die Arbeitsgruppe (AG) Informations- und Cybersicherheit der SIK in Zusammenarbeit mit der SIK-AG Cloud-Governance geplant, die mit der Nutzung von Cloud-Diensten einhergehenden Sicherheitsanforderungen in einer erweiterten Form der NSP-2017 als Anhang zu adressieren. Die Kantone sind darüber hinaus vom neuen Informationssicherheitsgesetz (ISG) betroffen. Dieses Gesetz soll den Rahmen für eine sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel abstecken. Dies bedeutet, dass auch Kantone im Umgang mit Daten oder beim Zugriff auf Informatikmittel des Bundes eine mindestens gleichwertige Informationssicherheit gewährleisten müssen. In Zusammenarbeit mit dem VBS und anderen Partnern aus den Kantonen (RK MZF und PTI) kümmert sich A. Gutknecht, der Vorsitzende der Arbeitsgruppe Informations- und Cybersicherheit der SIK, um eine fachgerechte Information und einen Austausch zum neuen Gesetz. Insbesondere geht es um die Betroffenheit der Kantone im Rahmen des ISG zu klären und die nötigen Sicherheitsanforderungen daraus abzustimmen. Das ISG soll am 1. April 2023 in Kraft treten.

Handlungsfeld 5: Krisenmanagement

Im Rahmen des Projekts «**Cyberübung mit kritischen Infrastrukturen im Gesundheitssektor**» (Massnahme 17 der NCS «Gemeinsame Übungen zum Krisenmanagement») hat der SVS zusammen mit dem NCSC (Max Klaus, stv. Leiter Operativer Cybersicherheit OCS, und Pascal Lamia, Operativer Leiter), Markus Meile, Stabschef der städtischen Führungsorganisation der Stadt Zürich, und Balz Dürst, wissenschaftlicher Mitarbeiter, Bundeskanzlei, Sektion Strategische Führungsunterstützung (STF), im Dezember 2021 eine *Table-Top*-Übung (TTX) durchgeführt. Die Aktivitäten im Rahmen dieser Massnahme im vergangenen Jahr bezogen sich somit hauptsächlich auf die Vorbereitung der Übung. Konkret mussten eine Methode und die Ziele definiert und

entsprechend Anpassungen am Szenario vorgenommen werden. Wegen der Pandemie legte die Übungsleitung grossen Wert darauf, die Ressourcen des USZ nicht über die Massen zu beanspruchen. Die wichtigsten Erkenntnisse aus der Übung beziehen sich auf die Tragweite und die grosse Betroffenheit, die ein Cyberangriff auf das USZ erzeugen würde. Alle Abteilungen, Direktionen und Häuser des USZ wären ein Stück weit in die Bewältigung der Krise involviert. Darüber hinaus erkannten die Beübten, dass sowohl die Sensibilisierung der Geschäftsleitung und des Spitalrates als auch aller Mitarbeitenden kontinuierlich notwendig ist, um im Falle des Falles vorbereitet zu sein. Gegen Ende der Strategieperiode ist darauf aufbauend eine Stabsrahmenübung geplant, die die Beübten erneut mit einem Cyberangriff konfrontieren wird. Im Unterschied zur TTX werden weitere fiktive Elemente das Dringlichkeitsempfinden erhöhen.

Beim Konzept «Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation»[4], das im Rahmen der Massnahme 8 zur «**Schaffung der kantonalen Organisationen für Cybersicherheit**» von einer Arbeitsgruppe des SVS erarbeitet wurde, handelt es sich um dessen Herzstück. Nach seiner Verabschiedung durch die KKJPD im November 2020 wurde es in verschiedenen Gremien durch den Delegierten SVS präsentiert und diskutiert. Erwähnenswert sind insbesondere die Vorstellung im Cyberboard und ein Workshop an der Cyber-Landsgemeinde von 2021, den der Delegierte SVS zusammen mit Florian Schütz, dem Delegierten des Bundes für Cybersicherheit, leitete. In der vergangenen Berichtsperiode zeigte sich, dass mehrere Kantone sich Gedanken zu ihrer Organisation im Bereich der Cybersicherheit machen. Einige von ihnen haben bereits konkrete Schritte eingeleitet. So inserierte zum Beispiel der Kanton Luzern im Herbst 2021 erstmals die Stelle eines oder einer kantonalen Cyberdelegierten, aber auch der Kanton Zürich liess vernehmen, dass sein Amt für Informatik gemäss diesem Konzept zusammen mit der Kantonspolizei Zürich, der Staatsanwaltschaft sowie dem Bevölkerungsschutz an einem Vorschlag für eine kantonale Cyberorganisation arbeite. Im Verlauf des Jahres 2022 wird das bestehende Konzept erstmals aktualisiert und mit Beispielen aus den Kantonen ergänzt. Um ein vollständiges Bild über «die kantonale Cyberorganisation» zu erhalten, zeigt sich eine Umfrage an.

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). Am 16. September 2021 fand die 9. Cyber-Landsgemeinde statt, 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. In den Diskussionen ging es insbesondere um den Fall eines konkreten Cyberangriffs und die Bewältigung dessen sowie um Fragen der digitalen Identität. 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 Cyberstrukturen, wie sie der Bundesrat im Januar 2019 verabschiedet hat, präsentieren sich wie folgt:

[4] Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation, Sicherheitsverbund Schweiz (2021)

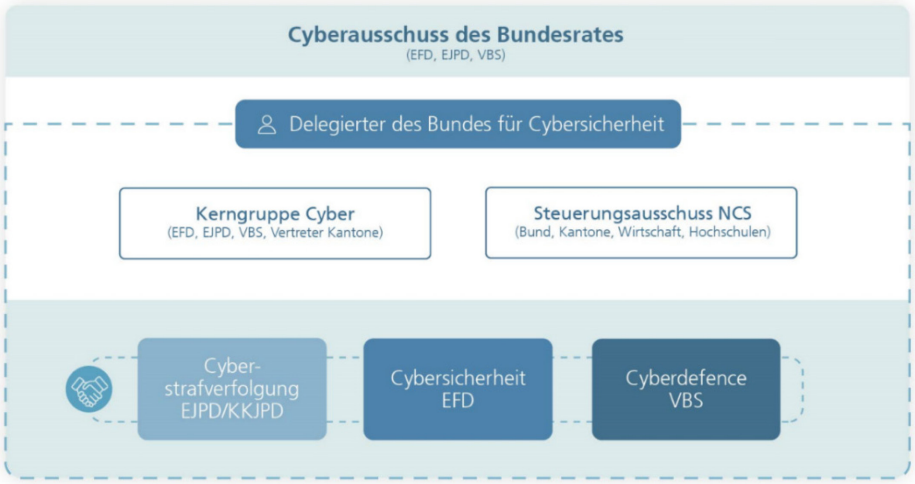

Abbildung I: Organisation des Bundes im Bereich Cybersicherheit (Quelle: NCSC)

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 SVS und der Delegierte des Bundes für Cybersicherheit, der seit August 2019 in dieser Funktion tätig ist und die Aufgabe hat, zum Schutz der Schweiz vor Cyberrisiken eine optimale Koordination der Arbeiten der Kantone und des Bundes sicherzustellen, haben ihren Austausch im vergangenen Jahr fortgesetzt. Auch die enge Zusammenarbeit zwischen dem SVS und dem Nationalen Zentrum für Cybersicherheit (NCSC) kam im Rahmen verschiedener Arbeiten zum Ausdruck.

Im Zusammenhang mit dem Mandat im Hinblick auf ein Kompetenznetzwerk Cyber, das der SVS im März 2020 von seiner Politischen Plattform erhalten hatte, ergab die vom SVS durchgeführte Erhebung, dass im Bereich Cybersicherheit ein grosses Aus- und Weiterbildungsangebot besteht. Der SVS erarbeitete anschliessend in Zusammenarbeit mit dem Cyber-Defence Campus der armasuisse und der Militärakademie eine **Übersicht über diese Bildungsangebote an Schweizer Universitäten und Hochschulen**. Diese wurde im November 2021 auf der Website des NCSC veröffentlicht[5] und im Februar 2022 aktualisiert.

Der SVS wurde in die Arbeiten des NCSC zur Umsetzung der Massnahme 9 der NCS 2018–2022 (Prüfung einer **Meldepflicht** für Cyber-Vorfälle und Entscheid über Einführung) einbezogen. Behörden gehören gemäss der Nationalen Strategie zum Schutz kritischer Infrastrukturen zu einem kritischen Teilsektor, weshalb Kantons- und Gemeindebehörden der Meldepflicht unterstehen werden. Darüber hinaus haben viele der meldepflichtigen Unternehmen kantonale oder kommunale Trägerschaften. In diesem Sinne hat der Delegierte SVS an mehreren Sitzungen des Koordinationsausschusses zur Einrichtung einer Meldepflicht teilgenommen, welche durch die Geschäftsstelle des NCSC geleitet waren. Zur Vorlage für die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen, zu der auch der SVS einen Beitrag leisten soll, wurde die Vernehmlassung eröffnet, die bis Mitte April 2022 dauert. Die Vorlage schafft die gesetzlichen Grundlagen für die Meldepflicht und definiert die Aufgaben des NCSC, welches als zentrale Meldestelle für Cyberangriffe vorgesehen ist. Der Bundesrat will das Meldewesen stärken, indem er die Betreiberinnen und Betreiber kritischer Infrastrukturen verpflichtet, dem NCSC Cyberangriffe zu melden. Über die Meldepflicht soll sichergestellt werden, dass das NCSC aufgrund der umfassenden Informationen über ein

[5] Übersicht der Schweizer Bildungsangebote im Cyberbereich

übersichtlicheres Lagebild verfügt, die Bedrohungslage einschätzen und aktuelle Angriffsmuster frühzeitig erkennen und dadurch andere Betreibende kritischer Infrastrukturen frühzeitig vor Cyberangriffen warnen kann.

Der Umsetzungsplan zur NCS 2018–2022 sah im Rahmen des strategischen Controllings eine **Wirksamkeitsüberprüfung** bis Ende 2022 vor. Das NCSC hat dazu die beiden Forschungs- und Beratungsunternehmen econcept und EBP mandatiert. Als Mitglied im Steuerungsausschuss und massnahmenverantwortliche Stelle war der SVS in diesen Prozess involviert. Konkret wurden der Delegierte und die Geschäftsstelle im Interview unter anderem zur Zweckmässigkeit und Angemessenheit der NCS 2018–2022 im Angesicht der Herausforderungen im Cyberbereich befragt. Der Bericht wird bis zum Ende des 1. Quartals 2022 abgeschlossen sein.

5. Weitere Aktivitäten der Geschäftsstelle des Delegierten SVS

Der SVS war in der Berichtsperiode in verschiedene Aktivitäten involviert, die sich aus der Umsetzung des NCS 2018–2022 ergaben. Es handelte sich dabei insbesondere um Projekte, die im Umsetzungsplan der Kantone zur NCS vorgesehen sind.

Ferner intensivierte sich im Berichtszeitraum die Zusammenarbeit zwischen dem SVS und dem Swiss Support Center for Cybersecurity (SSCC). Das SSCC hatte bereits an einer Sitzung der Fachgruppe Cyber des SVS im Dezember 2020 seine Aufgaben und Rolle näher vorgestellt. Es hat sich vorgenommen, als Vermittlerin für Anfragen von öffentlicher Seite im Bereich der Cybersicherheit zu walten und dabei sein besonderes Netzwerk im akademischen Bereich zur Verfügung zu stellen. In einem vom SSCC organisierten Webinar im Mai 2021 gab der Delegierte ein Einführungsreferat zur Sicherheit von Software-Lieferketten («Software Supply Chain Security»). Ein weiteres Webinar haben das SSCC und der SVS zusammen zum Thema «Ransomware Attacks» organisiert, das von mehr als 100 Teilnehmenden aus verschiedensten Disziplinen, von Akademie, über Behörden und Privatwirtschaft, mitverfolgt wurde. Es fand am 23. November 2021 statt. Das SSCC hat wiederholt sein Fachwissen eingebracht, um die im Umsetzungsplan der Kantone definierten Massnahmen inhaltlich zu unterstützen und mit eigenen Projektideen zu ergänzen.

Das Thema Cyberangriffe, unter anderem durch Ransomware, beschäftigt die Gemeinden stark. Der SVS und der Schweizerische Gemeindeverband haben einen Austausch initiiert, in dem es um den Schutz der Gemeinden vor Cyberangriffen geht und der im Laufe der Zeit eine oder mehrere Schutzlösungen für die Gemeinden hervorbringen soll. Auch wird möglicherweise demnächst eine Bestandsaufnahme der Organisation der Schweizer Gemeinden im Umgang mit solchen Bedrohungen erstellt.

Mit der Armee und anderen betroffenen Stellen ist der SVS in einen Dialog getreten, um zu eruieren, wie die Kantone in der Organisation von Cyberübungen unterstützt werden könnten.

Schliesslich wurde der Delegierte SVS angefragt, im Beirat des Projekts «Trust Valley» mitzuwirken, das auf Initiative der Kantone Waadt und Genf entstand und das Know-how der Genferseeregion im Bereich Digital Trust und Cybersicherheit fördern soll. In einer gemeinsamen Initiative unterstützen die öffentliche Hand, akademische Institutionen und Wirtschaftsakteure dieses einzigartige Kompetenzzentrum und begünstigen die Entstehung innovativer Projekte.

6. Bilanz und Ausblick

Die Arbeiten zur Umsetzung der Projekte wurden dank dem Engagement der Projektverantwortlichen auch in der Berichtsperiode fortgesetzt. Trotz der verschiedenen Einschränkungen im Zusammenhang mit der Covid-19-Pandemie, die sich zuvor auf den Fortschritt der Arbeiten ausgewirkt hatten, ist die Umsetzung im Allgemeinen zufriedenstellend. Die Kantone haben somit den Schutz ihrer Verwaltung und der Bevölkerung vor Cyberrisiken verbessert.

In der Berichtsperiode verstärkte sich zudem die Zusammenarbeit zwischen dem NCSC und den Kantonen, insbesondere im Rahmen der Reflexionen zu den neuen strategischen Zielen der dritten NCS, zumal die Kantone noch besser darin einbezogen sein sollen. Die Kantone werden darüber hinaus vom SVS kontaktiert, der zusammen mit seinen VertreterInnen die Umsetzung der dritten NCS auf kantonaler Ebene koordiniert. Die Fachgruppe Cyber des SVS wird im Übrigen im Laufe des Jahres 2022 drei- statt zweimal zu einer ordentlichen Sitzung zusammenkommen.

Die Umsetzung der verschiedenen Projekte ist bis Ende 2022 gemäss Zeitplan soweit möglich voranzutreiben. In Zukunft soll zudem die Zusammenarbeit mit dem Beauftragten von Bund und Kantonen für die Digitale Verwaltung Schweiz vertieft werden, zumal die DVS die Aktivitäten der SIK übernommen hat.