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 (NCS II)

März 2020

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 elf Monate seit dessen Verabschiedung im April 2019 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, stellvertretender 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 • Bestandsaufnahme der in den Kantonen vorhandenen Weiterbildungen • Erstellung des Weiterbildungskonzepts • Präsentation des Konzepts an der Vorstandsversammlung der KKJPD	• Beschlussfassung in der Frühjahrsversammlung der KKJPD am 2. April 2020 • Bildung eines Steuerungsausschusses und einer Arbeitsgruppe • Detailplanung • Kick-Off
Bedrohungslage	(2) #MISP – Malware Information Sharing Platform von MELANI für und mit den Kantonen	Marc Barbezat, Leiter Digitale Sicherheit des Kantons Waadt, in Zusammenarbeit mit MELANI	• 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	• Bestandsaufnahme der bestehenden Taxonomien und Vorbereitung einer einheitlichen Taxonomie zu den Cyberbedrohungenn • Erarbeitung eines Ansatzes zur Einrichtung und Weiterentwicklung eines Monitoringprozesses mit Hilfe von OSINT • Die Kantone haben Zugang zum Lageradar von MELANI • Begleitung der Kantone bei der aktiven Nutzung der Informationen vom Lageradar von MELANI	• Begleitung der Kantone bei der aktiven Nutzung der Informationen vom Lageradar von MELANI • Begleitung der Kantone bei der Einrichtung eines Monitoringprozesses mit Hilfe von OSINT
Resilienzmanagement	(3) Erhebungstool zur Verbesserung der IKT-Resilienz in den Kantonen	Max Haefeli, stellvertretenden Leiter Kantonale 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 Kantone	• Die Kantone führen die Erhebung durch • Die Resultate werden von der Projektleitung ausgewertet • Die anonymisierten Resultate werden bestimmten Fachgremien und Konferenzen (SIK, KKJPD) präsentiert
	(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.	• Die Arbeitsgruppe hat vom Umsetzungsplan der Kantone zur NCS II und dem Projekt Kenntnis genommen.	
	(5) Sensibilisierung der Bevölkerung für Cyberrisiken	Chantal Billaud, Geschäftsleiterin der Schweizerischen Kriminalprävention (SKP)	• Etablierung und Konsolidierung einer Partnerschaft für die Sensibilisierung der jungen und älteren Menschen • 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 weiteren, zugeschnittenen Lerninhalten innerhalb der jeweiligen Arbeitsgruppen

Handlungsfelder	Name des Projekts	Umsetzungsverantwortung	Messbare Ziele (gemäss Umsetzungsplan der Kantone)	Erreichte Meilensteine	Ausblick/Folgearbeiten
				• Die verschiedenen Arbeitsgruppen haben bereits erste Projekte zur Sensibilisierung der Bevölkerung gemeinsam erarbeitet und entsprechende Produkte veröffentlicht.	
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). Durch diesen Vergleich werden die Handlungsfelder definiert und priorisiert. • Umsetzung in sechs Kantone die kantonseigene NSP anhand der NSP-SIK 2017	• Neun Kantone setzen ihre kantonseigene NSP um (auf der Basis von jener der SIK 2017)
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 eines Universitätsspitals und weiterer Partner zur Durchführung einer Übung	• Zusammensetzung der Arbeitsgruppe
	(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	• Erstellung des ersten Entwurfs des Konzepts zur Cyberorganisation • Besprechung des Konzepts in der Arbeitsgruppe	• Fertigstellung des Konzepts zur Cyberorganisation • Präsentation des Konzepts in der KKJPD
Aussenwirkung und Sensibilisierung	(9) Aktive Kommunikation zu den Tätigkeiten der Kantone im Rahmen der NCS II	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 • Publikation des Jahresbericht zum Stand der Projekte aus dem Umsetzungsplan der Kantone zur NCS II	• SVS organisiert die 8. Cyberlandsgemeinde, die das Ziel verfolgt, über die Fortschritte bei den Projekten des Umsetzungsplans der Kantone zur NCS II zu informieren

1. Einleitung

Der Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022 (NCS II) 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 Cybersicherheit des SVS.

Der Umsetzungsplan der Kantone ist integrierender Bestandteil des Umsetzungsplans des Bundes zur NCS II 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 Cybersicherheit des SVS sowie auch im Steuerungsausschuss NCS II vertreten. Dessen Aufgabe ist das gemeinsame Projektmanagement. Er stellt die koordinierte, zielgerichtete Umsetzung der NCS-Massnahmen sicher. Seit April 2019 ist er zweimal zusammengekommen.

Der Umsetzungsplan der Kantone zur NCS II sieht 13 Projekte in sieben der zehn Handlungsfelder der NCS II 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 sind eine Projektleiterin oder ein Projektleiter aus den Kantonen für die Umsetzung verantwortlich, sie werden vom SVS unterstützt. Die Umsetzung der jeweiligen Projekte basiert auf einem Zeitplan, den die Arbeitsgruppe des SVS am 7. Mai 2019 für angemessen erachtete und gewissen Handlungsspielraum offenlässt.

2. Fachgruppe Cybersicherheit des Sicherheitsverbunds Schweiz

Die Fachgruppe Cybersicherheit 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, die Koordinationsstelle NCS und der Delegierte des VBS für Cyberdefence. Nach der Verabschiedung der NCS II und des Umsetzungsplans der Kantone wurden Auftrag und Zusammensetzung der Fachgruppe Cybersicherheit 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 zweimal 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 Steuerungsausschuss der NCS II zu, dem sowohl der Delegierte des SVS als auch der Generalsekretär der KKJPD formell angehören.

3. Umsetzungsstand der Projekte

Handlungsfeld 1: Kompetenzen- und Wissensaufbau

Die Kantone haben eine generelle Stärkung der Cyberkompetenzen ihrer Mitarbeitenden beschlossen. Mit dem Projekt **«Entwicklung eines Weiterbildungskonzepts und -moduls für kantonale Verwaltungen»** (Massnahme 2 der NCS II «Ausbau und Förderung von Forschungs- und Bildungskompetenz») soll den kantonalen Verwaltungen ein umfassendes und auf das Verwaltungspersonal zugeschnittenes Weiterbildungsprogramm zur Verfügung gestellt werden. Das Weiterbildungskonzept könnte auch sämtlichen Angestellten von Gemeindeverwaltungen und dem Personal der eidgenössischen Departemente angeboten werden. Sébastien Jaquier, stellvertretender Leiter des *Institut de lutte contre la criminalité économique (ILCE)* der *Haute école de gestion Arc* in Neuenburg, leitet die Arbeitsgruppe, die sich aus Informationssicherheitsbeauftragten von Bund und Kantonen zusammensetzt. Die Arbeitsgruppe hat eine partielle Bestandsaufnahme der in den Kantonen vorhandenen Weiterbildun-

gen (einschliesslich E-Learning) vorgenommen, die entweder spezifisch für die kantonale Verwaltung entwickelt wurden oder auf kommerziellen Lösungen basieren (z. B. IS-Fox, ESEC, Wombat, Kaspersky). Auf dieser Grundlage wurde das Weiterbildungskonzept erstellt und in der Folge vom Vorstand der KKJPD am 6. März 2020 genehmigt.

Handlungsfeld 2: Bedrohungslage

Zur Verbesserung ihrer Fähigkeiten der Beschreibung und Beurteilung von Cyberbedrohungen in der Schweiz haben die Kantone die Entwicklung und Einführung verschiedener Instrumente vorgesehen, mit denen Eindringversuche und Malware abgewehrt werden können. Mit dem Projekt **«#MISP – Malware Information Sharing Platform von MELANI für und mit den Kantonen»** wird Massnahme 4 der NCS II «Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyberbedrohungslage» umgesetzt.
Marc Barbezat, Leiter Digitale Sicherheit des Kantons Waadt, leitet die Projektumsetzung in Zusammenarbeit mit der Melde- und Analysestelle Informationssicherung (MELANI). Zusätzlich zum Lageradar von MELANI, zu dem alle Kantone Zugang haben (mindestens zur statischen Version), sollen die Kantone das Open-Source-Tool MISP kennen, nutzen und speisen. MISP ermöglicht den Informationsaustausch zu Anzeichen von Eindringversuchen und hat die bessere Erkennung von Cyberbedrohungen zum Ziel. Die Plattform ist zu einer Referenz geworden, weil sie vor allem von MELANI umfassend gespeist wird. Derzeit tauschen rund zehn Kantone über dieses Netzwerk aktiv operative Informationen zu Malware aus. Marc Barbezat begleitet die Kantone laufend (Sensibilisierung, Information) bei der aktiven Nutzung von MISP. Die Nutzung und die Stärkung dieses Instruments variiert von Kanton zu Kanton beachtlich, je nach Verfügbarkeit von Fachleuten und finanziellen Ressourcen. Für eine optimierte Nutzung der Instrumente ist eine gemeinsame Taxonomie nötig, mit der die Cyberbedrohungen schweizweit (auf Ebene Bund, Kantone, Gemeinden) kohärent und einheitlich strukturiert werden können. Marc Barbezat hat die bestehenden Taxonomien (NIST, ENISA, MITRE) analysiert und zur Vorbereitung eines einheitlichen Vokabulars zu den Cyberbedrohungen mit diversen Partnern des Bundes Gespräche geführt.

Handlungsfeld 3: Resilienzmanagement

Für die Verbesserung ihrer IKT-Resilienz haben die Kantone in ihrem Umsetzungsplan drei Projekte vorgesehen.

Mithilfe eines Erhebungstools sollen die Kantone die erforderlichen minimalen Anforderungen in Bezug auf Prozesse, Kompetenzen und Aufgaben analysieren. Das Instrument wurde von Max Haefeli, dem stellvertretenden Leiter Kantonale Informationssicherheit (Deputy CISO) des Kantons Basel-Stadt, erarbeitet und basiert auf dem Analyse-Tool «Minimalstandard zur Verbesserung der IKT-Resilienz» des Bundesamts für wirtschaftliche Landesversorgung (BWL). Max Haefeli zeichnet in Zusammenarbeit mit dem SVS, dem BWL und der Schweizerischen Informatikkonferenz (SIK) verantwortlich für das Projekt **«Erhebungstool zur Verbesserung der IKT-Resilienz in den Kantonen»** (Massnahme 5 der NCS II «Verbesserung der IKT-Resilienz der kritischen Infrastrukturen»). Projektziel ist, dass die Kantone Defizite in Bezug auf die IKT-Resilienz feststellen und beurteilen und darauf basierend gezielte Sicherheitsmassnahmen zur Risikominderung und zur Stärkung ihrer Sicherheitsorganisation ergreifen. Im Januar 2020 wurde den Kantonen das Erhebungstool zur Verfügung gestellt. Bis Anfang April 2020 sollen die zuständigen Stellen die Analyse durchführen.

Zur weiteren Verbesserung der IKT-Resilienz planen die Kantone die Förderung ihrer Zusammenarbeit durch die Institutionalisierung des Erfahrungsaustauschs und des Dialogs. Zur Umsetzung der NCS II und namentlich deren Massnahme 7 («Erfahrungsaustausch und Schaffung von Grundlagen zur Stärkung der IKT-Resilienz in den Kantonen») sieht der Umsetzungsplan das Projekt **«Verstärkter Erfahrungsaustausch über die Schweizerische Informatikkonferenz (SIK) mit der Schaffung von Grundlagen»** vor. Die Projektverantwortung liegt gemäss Umsetzungsplan bei der Arbeitsgruppe Informatiksicherheit der SIK in Zusammenar-

beit mit den federführenden kantonalen Regierungsstellen und deren Informationssicherheitsbeauftragten. Die Arbeitsgruppe Informatiksicherheit der SIK hat vom Umsetzungsplan der Kantone zur NCS II und dem erwähnten Projekt Kenntnis genommen, und in den nächsten Sitzungen sollen die nächsten Ziele definiert werden.

Beim Projekt **«Sensibilisierung der Bevölkerung für Cyberrisiken»**[1] soll zur Verbesserung der Resilienz der Schweiz in Bezug auf Cyberrisiken die Prävention in der Bevölkerung verstärkt werden. Chantal Billaud, Geschäftsleiterin der Schweizerischen Kriminalprävention (SKP), ist Projektverantwortliche. Zur Festlegung der geeigneten Strukturen und Gefässe für die Umsetzung effizienter Präventionsmassnahmen wurde ein erstes Austauschtreffen mit Vertreterinnen und Vertretern von Bund, Kantons- und Stadtpolizei organisiert. Auf der Grundlage der Diskussionen wurden verschiedene Gruppen (Kerngruppe, Austauschgruppe und Arbeitsgruppen) geschaffen, die ihre Tätigkeit aufgenommen haben. Einige Arbeitsgruppen haben bereits erste Produkte zur Sensibilisierung der Bevölkerung erarbeitet und veröffentlicht, wie nachfolgend dargelegt wird. Alle Projekte und Massnahmen wurden in Zusammenarbeit mit dem Netzwerk Ermittlungsunterstützung Digitale Kriminalitätsbekämpfung (NEDIK) lanciert.

- Arbeitsgruppe «Cyberweiterbildung Polizei» (Leitung: SKP): Die SKP ermittelte in einer Umfrage den Bedarf für eine Weiterbildung mit dem Ergebnis, dass Interesse besteht.
- Arbeitsgruppe «Filme» (Leitung: Waadtländer Kantonspolizei und Konferenz der Polizeikommandanten der Westschweiz, Bern und Tessin [CCPC RBT]): Kurze Präventionskampagnen zum Thema Betrug im Internet (Kleinanzeigen-Betrug, Liebesbetrug [*Romance scams*] und Phänomen der *Money Mules* [Geldkuriere]) wurden 2019 über die Social-Media-Kanäle der Polizeikorps und der SKP veröffentlicht. Die Swiss Internet Security Alliance trägt die Präventionskampagnen der Polizeikorps mit und verbreitet sie über ihre Website (ibarry.ch) sowie ihre Social-Media-Kanäle.
- Arbeitsgruppe «Material KMU» (Leitung: Kantonspolizei Bern und MELANI): Im Februar 2020 wurden eine Broschüre sowie Präventionsmaterial veröffentlicht, das sich spezifisch an KMU richtet.
- Arbeitsgruppe «Nationale Melde- und Präventionsseite» (Leitung: NEDIK und Kantonspolizei Zürich in Zusammenarbeit mit MELANI): Die Zürcher Kantonspolizei hat im November 2019 die Website cybercrimepolice.ch mit aktuellen Warnungen für die Bevölkerung zu Cybercrime-Delikten ins Leben gerufen.

Handlungsfeld 4: Standardisierung/Regulierung

Die Kantone haben die 2017 von der SIK erstellte Netzwerksicherheitspolicy verabschiedet (allen Mitgliedern der SIK im Intranet zugänglich). Sie sehen im Rahmen der Massnahme 8 der NCS II «Entwicklung und Einführung von Minimalstandards» vor, die Standards der **Netzwerksicherheitspolicy der SIK** auf kantonaler Ebene umzusetzen. Der Leiter der Arbeitsgruppe Informatiksicherheit der SIK, Adrian Gutknecht, führt dieses Projekt und arbeitet dabei mit dem Kompetenzzentrum Polizeitechnik (PTI) zusammen.
2018 wurden Vorgaben für die Umsetzung der Netzwerksicherheitspolicy in den Kantonen erarbeitet und von der SIK verabschiedet. Heute haben sechs Kantone eine kantonseigene Netzwerksicherheitspolicy (in Anlehnung an jene der SIK von 2017) umgesetzt, und neun Kantone planen die Umsetzung 2020. Die Implementierung der Standards der Netzwerksicherheitspolicy in den Kantonen erfordert technische und architektonische Anpassungen an den Netzwerkinfrastrukturen, was sich auf die kantonalen Budgetplanungen auswirkt. Der Umsetzungsgrad in den Kantonen ist deshalb teilweise von diesen langfristigen Prozessen abhängig.

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

Handlungsfeld 5: Krisenmanagement

Der Umsetzungsplan der Kantone sieht zur Massnahme 17 der NCS II «Gemeinsame Übungen zum Krisenmanagement» ein Projekt mit dem Titel **«Cyberübung mit kritischen Infrastrukturen im Gesundheitssektor»** vor. Ziel dieses Projekt ist zunächst die Durchführung einer *Table-Top*-Übung mit Cyberaspekten in einer kritischen Infrastruktur im Gesundheitssektor sowie anschliessend einer Stabsrahmenübung, während denen die Führungsstrategie erprobt und die operative Koordination zwischen Bund, Kantonen und Betreibern der kritischen Infrastrukturen sowie den betroffenen Stellen überprüft wird.
Zunächst musste eine kritische Infrastruktur bezeichnet werden, in diesem Fall ein Universitätsspital. André Duvillard, Delegierter des SVS und Projektverantwortlicher, steht mit dem Universitätsspital Zürich, das sein Interesse an der Umsetzung dieses Projekts signalisiert hat, in Kontakt. Gespräche zur Zusammensetzung einer Arbeitsgruppe, die das Referenzszenario ausarbeiten wird, sind im Gange.

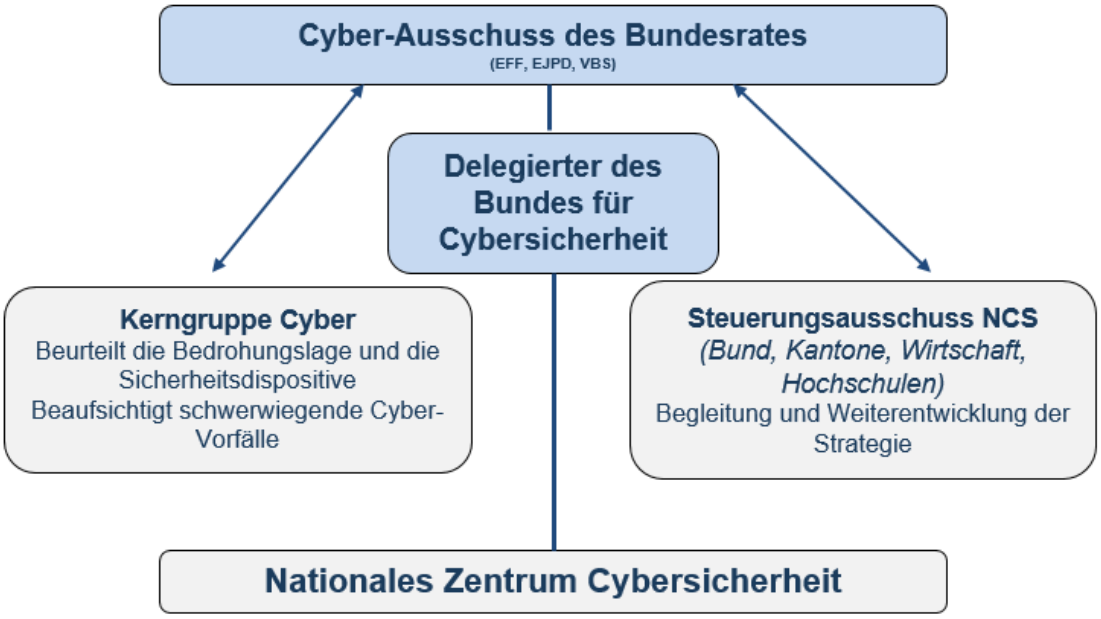
Das Projekt **«Schaffung der kantonalen Organisationen für Cybersicherheit»** bezweckt die Ausarbeitung eines Organisationsmodells zur Einführung in den Kantonen, mit dem die verschiedenen Aspekte der Cybersicherheit koordiniert werden können. Die Arbeitsgruppe des SVS unter der Leitung vom Delegierter des SVS setzt sich aus Vertreterinnen und Vertretern der Kantone Basel-Stadt, Freiburg, Genf, Tessin und Zürich zusammen. Sie erstellt in einem ersten Schritt ein Konzept als Richtlinie und Vorlage für die Kantone. Dieses wird voraussichtlich im Frühling 2020 fertiggestellt und im Laufe des Jahres der KKJPD vorgelegt. Bei der Erarbeitung des Konzepts hat die Arbeitsgruppe verschiedene Herausforderungen und Bedürfnisse angetroffen. Aus diesem Grund kann das Konzept zur kantonalen Modell-Organisation, aber auch die Auffassung und der Umfang der Weisungsbefugnis eines oder einer allfälligen kantonalen Cyberdelegierten und ihrer/seiner organisationalen Ansiedlung und Unterstellung je nach Kanton unterschiedlich ausgestaltet werden. Nichtsdestotrotz wird das Konzept den zuständigen kantonalen Behörden den Reflexionsprozess bei der Entwicklung einer passenden Cyberorganisation erleichtern.

Handlungsfeld 6: Aussenwirkung und Sensibilisierung

Die Kantone haben bei der Erstellung des Umsetzungsplans Interesse daran gezeigt, dass ihre Aktivitäten im Rahmen der NCS II sichtbar sind. Sie haben im Umsetzungsplan deshalb ein Projekt **«Aktive Kommunikation zu den Tätigkeiten der Kantone im Rahmen der NCS II»** vorgesehen (Massnahme 28 der NCS II «Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS»). Der SVS, dessen Delegierter die Projektverantwortung trägt, sorgt auf seiner Website (svs.admin.ch) für die Sichtbarkeit der Tätigkeiten der Kantone im Rahmen der NCS II. Ein neuer Reiter «Aktualitäten» wurde aufgeschaltet, wo aktuelle Meldungen aus den Kantonen zu ihren Tätigkeiten im Cyberbereich publiziert werden können. Die Seite wird regelmässig aktualisiert. Der SVS organisiert ausserdem die 8. Cyberlandsgemeinde, die 2020 stattfinden wird und – wie dieser Bericht – das Ziel verfolgt, über die Fortschritte bei den Projekten des Umsetzungsplans der Kantone zur NCS II zu informieren.

4. Einbindung der Kantone in die Cyberstrukturen des Bundes

Das Jahr 2019 war geprägt durch den Aufbau der Cyberstrukturen des Bundes, wie sie der Bundesrat im Januar 2019 auf der Grundlage seines Entscheids vom 4. Juli 2018 verabschiedet hat.



Die Ernennung des Delegierten des Bundes für Cybersicherheit ermöglichte den verschiedenen Instanzen, ihre Tätigkeiten nach und nach aufzunehmen und die Kantone systematisch einzubeziehen. So wurde der Präsident der KKJPD zur ersten Sitzung des Cyberausschusses des Bundesrates eingeladen. Auf der anderen Seite bindet der SVS den Delegierten des Bundes für Cybersicherheit seit dessen Amtsantritt in seine Aktivitäten im Cyberbereich ein.

Das Nationale Zentrum Cybersicherheit befindet sich noch in der Entwicklungsphase. Sein genaues Tätigkeitsfeld wird in den nächsten Monaten zu bestimmen sein. Mehrere Kantone haben bereits ihr Interesse an einer Mitwirkung im Rahmen von Projekten, die sie entwickeln, signalisiert. Im August und im November 2019 fanden zwei Runde Tische unter der Leitung von Bundesrat Ueli Maurer, dem Vorsteher des Eidgenössischen Finanzdepartements (EFD), statt.

5. Weitere Aktivitäten der Geschäftsstelle des Delegierten SVS

Dank der Projekte zur NCS I und der in den letzten Jahren hergestellten Kontakte hat die Geschäftsstelle des Delegierten SVS ein grosses Netzwerk im Cyberbereich aufbauen können, das sowohl die Ebenen Bund, Kantone, Gemeinden als auch die kritischen Infrastrukturen umfasst. Dadurch hat sie einerseits einen guten Überblick über die Herausforderungen und kann andererseits auch ihre Rolle als strategische Schnittstelle zwischen den Kantonen und dem Bund wahrnehmen.

Als Mitglied der Cyberexpertengruppe des VBS und der strategischen Plattform des Cyberboards verfügt der Delegierte des SVS seinerseits über einen guten Überblick über die Herausforderungen in den drei Tätigkeitsbereichen Cybersicherheit, Cyberabwehr und Cyberkriminalität. Obwohl unser föderalistisches System zahlreiche Koordinationsstrukturen vorgibt, sind in den letzten fünf Jahren unbestritten Fortschritte erzielt worden, die zu einer besseren Berücksichtigung der Interessen und Bedürfnisse der verschiedenen institutionellen Akteure führten.

6. Bilanz und Ausblick

Mit der Verabschiedung des Umsetzungsplans der Kantone zur NCS II haben diese klar ihren Willen ausgedrückt, in Eigenverantwortung und Eigeninitiative den Schutz der Bevölkerung vor Cyberrisiken zu stärken. Gewisse Herausforderungen in Zusammenhang mit den unterschiedlichen bestehenden Strukturen, Ressourcen und Personalbeständen in den Kantonen haben die Umsetzung der Projekte zwar auf die Probe gestellt. Doch sind die verzeichneten

Fortschritte trotz gewisser Schwierigkeiten insgesamt zufriedenstellend. Die meisten im Umsetzungsplan der Kantone vorgesehenen Projekte wurden aufgegleist, und der Zeitplan kann im Grossen und Ganzen eingehalten werden. Das Engagement der Projektverantwortlichen, die mehrheitlich aus den kantonalen Strukturen kommen, und ihre fruchtbare Zusammenarbeit mit dem SVS tragen massgeblich dazu bei, dass die Umsetzung der Projekte bereits weit fortgeschritten ist.

2020 sind die verschiedenen Projekte gemäss Zeitplan voranzutreiben. Insbesondere sind die Interessen und Bedürfnisse der Kantone systematisch zu berücksichtigen, denn die Kantone sind ein unverzichtbarer Akteur in der Cybersicherheit.

Schliesslich muss im Hinblick auf die künftige Rolle der Kantone ein Projekt spezifisch erwähnt werden, nämlich deren Beitrag zum Nationalen Zentrum Cybersicherheit. Im Nachgang zu den zwei unter Ziffer 4 erwähnten Runden Tischen wurde vereinbart, eine möglichst umfassende Bestandsaufnahme sämtlicher Projekte und Leistungen zusammenzustellen, die in den Kantonen – häufig in Zusammenarbeit mit der Wissenschaft und der Wirtschaft – entwickelt wurden. Diese soll dem Nationalen Zentrum Cybersicherheit und allen Kantonen als Referenzkatalog zur Verfügung stehen. Der Delegierte für Cybersicherheit und der Delegierte des SVS haben ein entsprechendes Konzept verfasst, das Anfang Januar 2020 an der Präsidienklausur der Konferenz der Kantonsregierungen (KdK) vorgestellt wurde. Dieses wurde mittels Mandat an den Delegierten des SVS formalisiert, welches die Politische Plattform SVS im März 2020 im Zirkularverfahren genehmigt hat.