Bericht zum Umsetzungsstand der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022

Stand zweites Quartal 2021

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Inhaltsverzeichnis

Vorwort

Seit dem letzten Umsetzungsbericht zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) 2018-2022 ist etwas über ein Jahr vergangen. «Wir sind auf Kurs», habe ich damals zusammengefasst. Das sind wir weiterhin – auch wenn ich gerne schon etwas weiter wäre in der Umsetzung. Mittlerweile sind gut zwei Drittel der Umsetzungszeit vorbei und rund 60 Prozent der Meilensteine sind realisiert. Es würde mir – schon rein mathematisch – noch besser gefallen, wenn bereits zwei Drittel umgesetzt wären. Tatsächlich ist der Abschluss der noch laufenden Meilensteine aber auf Ende dieses Jahres oder auf Ende 2022, also auf Ende der Laufzeit der NCS, geplant.

Je heterogener ein Vorhaben ist, desto wichtiger werden die Koordination und der Aufbau von klaren Strukturen. In Bezug auf die Umsetzung der NCS ist der Aufbau der Organisationsstrukturen im Bund deshalb ein zentrales Element. Mit der Inkraftsetzung der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung Mitte 2020 sind Rahmen und Zuständigkeiten klar und die Zusammenarbeit innerhalb der Bundesverwaltung sowie mit den Kantonen, der Wirtschaft und der Wissenschaft geregelt.

Für mich hat die Umsetzung der NCS im letzten Berichtszeitraum vom zweiten Quartal 2020 bis und mit Quartal zwei 2021 deutlich an Fahrt aufgenommen. Die Bereiche Cybersicherheit, Cyberdefence und Cyberstrafverfolgung haben sich strategisch und organisatorisch weiterentwickelt.

Der Ausbau des Nationalen Zentrums für Cybersicherheit (NCSC) wurde vorangetrieben und damit einhergehend weitere Dienstleistungen etabliert. Der Aufbau eines Schwachstellenmanagements wurde an die Hand genommen. In diesem Zusammenhang wurde unter anderem erfolgreich ein Pilotversuch durchgeführt, in welchem ethische Hacker beauftragt wurden, Schwachstellen in Systemen der Bundesverwaltung zu suchen. Solche sogenannten Bug Bounty Programme sollen künftig für die gesamte Bundesverwaltung etabliert werden. Im Rahmen der SwissCovid App und des Covid-Zertifkats führte das NCSC zwei Public Security Tests durch und konnte so seine Expertenleistung der Bundesverwaltung zur Verfügung stellen. Bei diesen öffentlichen Tests vorangehenden Private Security Test des Covid-Zertifikats wurde zugleich erstmals mit dem Nationalen Testinstitut für Cybersicherheit (NTC), das auf Initiative des Kantons Zug gegründet wurde, zusammengearbeitet.

Das VBS hat sich mit der Strategie Cyber VBS die Leitplanken für die strategische Ausrichtung im Bereich Cyberdefence gesetzt. Sie zeigt auf, wie sich das VBS in die übergeordnete NCS einbringt. Speziell zu erwähnen ist auch die immer weiter fortschreitende Etablierung des Cyber-Kommandos der Armee. Dieses wird eine wichtige Rolle in der Cyberdefence einnehmen. Das VBS hat überdies an diversen Cyberübungen teilgenommen und solche auch selber durchgeführt. Hierbei wurde jeweils der Kooperationsgedanke stark in den Vordergrund gestellt.

Im Bereich der Strafverfolgung wurden mittels Verwaltungsvereinbarung Organisation und Finanzierung des Netzwerks digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) geregelt. Das Netzwerk bündelt die Spezialressourcen national, um die digitale Kriminalität effizient zu bekämpfen und leistet einen wichtigen Beitrag zur Prävention. Der strategische Dialog über das Cyberboard zwischen Bundesanwaltschaft, Fedpol und den kantonalen Sicherheitsbehörden gewinnt zunehmend an Wichtigkeit, um die Strafverfolgung optimal auf die Zukunft auszurichten.

Uns bleiben noch anderthalb Jahre, die NCS umzusetzen. Es gibt noch einiges zu tun, und ich bin zuversichtlich, dass wir rasch weitere Fortschritte zu Gunsten der Bevölkerung, der Behörden, der Wirtschaft und der Wissenschaft erzielen werden. Klar ist, die Herausforderungen und Arbeiten im Bereich Cybersicherheit werden auch nach Beendigung der NCS 2018-2022 weitergehen, Abklärungen und Vorarbeiten im Hinblick auf die Folgestrategie wurden bereits initiiert.

1 Übersicht Stand der Umsetzungsarbeiten

Im Umsetzungsplan der NCS werden in den 29 Massnahmen 275 Meilensteine geführt. Bis im zweiten Quartal 2021 wurden 154 davon umgesetzt, 8 konnten nicht erreicht werden. 6 von 29 Massnahmen sind damit vollständig abgeschlossen. Der Umsetzungsstand wird in Kapitel 5 detailliert beschrieben. Die untenstehende Übersicht gibt einen Eindruck über den Stand der Umsetzung und die weitere Meilensteinplanung.

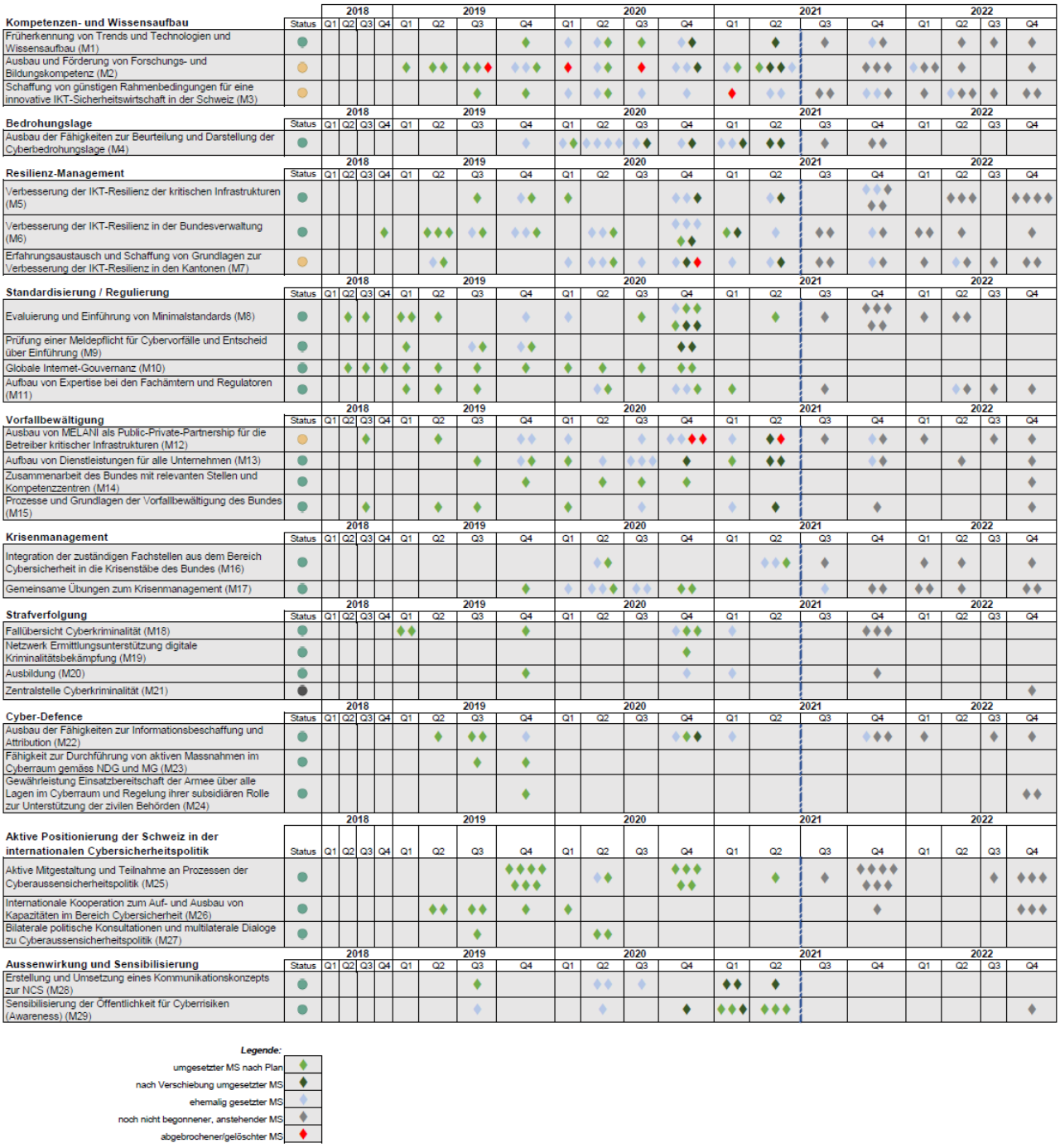


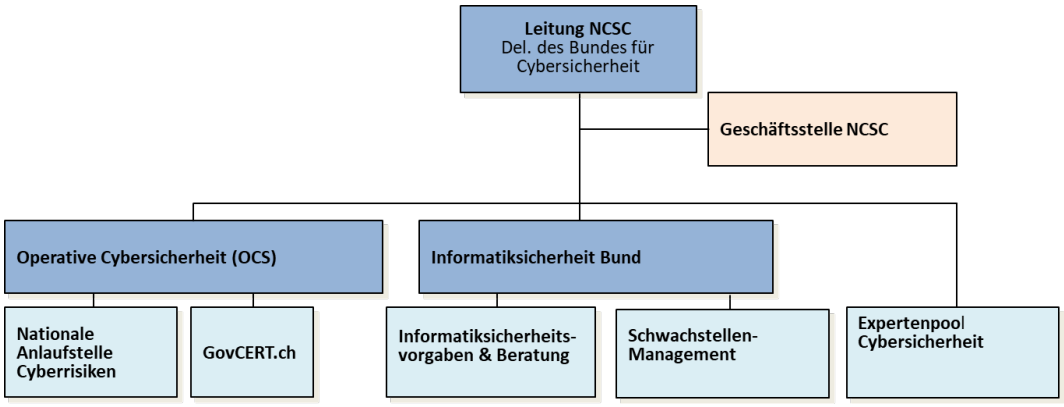
Abbildung 1 Übersicht Stand der Umsetzungsarbeiten

2 Organisation und Teilstrategien zur Umsetzung der NCS

Zur Umsetzung der NCS gehört der Aufbau der Organisationsstrukturen im Bund. Im Bericht zum Umsetzungsstand 2020 wurden die überdepartementalen Koordinationsgremien (Cyber-Ausschuss des Bundesrats, Kerngruppe Cyber und Steuerungsausschuss NCS) beschrieben. Diese Gremien haben ihre Arbeit weitergeführt und sich regelmässig getroffen. Im Folgenden wird auf die wichtigsten organisatorischen und strategischen Entwicklungen in den Bereichen Cybersicherheit, Cyberdefence und Cyberstrafverfolgung eingegangen.

2.1 Stand Aufbau NCSC

Der Aufbau des Nationalen Zentrum für Cybersicherheit (NCSC) wurde 2020 weiter vorangetrieben. Am 13. Mai 2020 hat der Bundesrat weitere 11 Stellen für das NCSC bewilligt. Aktuell (Mai 2021) besteht das NCSC aus 32 Mitarbeitenden, bis Ende 2021 werden 13 noch offene Stellen besetzt. Die Organisation des NCSC ist in Abbildung 1 dargestellt.



Das NCSC betreibt seit 1. Januar 2020 eine nationale Anlaufstelle für Cybervorfälle. Im Jahr 2020 gingen 10’834 Meldungen von Unternehmen und Bevölkerung ein. Bei den Meldungen mit klarer Cyberzuordnung handelte es sich in 5’924 Fällen (55 %) um Betrugsversuche, in 416 Fällen (4 %) wurde Schadsoftware gemeldet, 165 Vorfälle (2 %) betrafen Hacking und 24 (<1 %) Datenabflüsse.
Das technische Analyseteam des NCSC ist das GovCERT (Computer Emergency Response Team). Es hat in Zusammenarbeit mit Partnern 2020 7’500 Phishing-Seiten gestoppt, 4’500 Malware Incidents erfasst und dabei 90’000 infizierte IPs informiert und 177 Betreiber kritischer Infrastrukturen mit bedrohungsspezifischen Informationen versorgt.
Im Bereich der rechtlichen Vorgaben sind die Weisungen des Bundesrats zur IKT-Sicherheit in der Bundesverwaltung per 1. April 2021 in die Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) integriert worden. Mit diesem Schritt wurden die Vorgaben vereinfacht und gleichzeitig die Rolle des Delegierten für Cybersicherheit gestärkt. Der oder die Delegierte kann nun direkt Vorgaben zum Prozess und zur Dokumentation der Sicherheitsverfahren erlassen.[1]

[1] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/cyrv-vorgaben.html

2.2 Strategie Cyber VBS

Die Strategie Cyber VBS, welche von der Departementschefin des VBS im Frühjahr 2021 genehmigt wurde, bildet die Basis für die strategische Ausrichtung des Departements im Bereich Cyberdefence für die Jahre 2021-2024.[2] Sie zeigt auf, wie sich das VBS in die übergeordnete NCS einbringt, zum Schutz der Schweiz beiträgt, sie im Cyberraum verteidigt und die Handlungsfreiheit des Landes massgeblich erhöht. Sie beinhaltet alle nachrichtendienstlichen und militärischen Massnahmen zum Schutz der für die Sicherheit des Landes kritischen Systeme, zur Abwehr von Cyberangriffen, zur Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und zum Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden.
Bei der Umsetzung gilt der Grundsatz, dass sich alle Akteure mit cyberrelevanten Aufgaben im VBS aktiv im Rahmen der Strategie Cyber VBS koordinieren. Sie arbeiten eng zusammen, damit Risiken und Chancen identifiziert und gemeinsam bewältigt werden können. Dazu gehört, dass das Departement seine Entwicklung fachlich, materiell, prozessual, wie auch personell auf die durch die Cyberbedrohung bestehende Herausforderung ausrichtet. Insbesondere die Aus- und Weiterbildung aller VBS-Mitarbeitenden sowie des Militärs (Berufs- und Milizpersonal) ist von zentraler Bedeutung.
Zudem arbeiten die Cyberverantwortlichen im VBS zur Umsetzung der Massnahmen mit ihren Partnern zusammen. Neben dem NCSC, sind das die Kantone und Gemeinden, die Forschung und Privatwirtschaft, und auch internationale Organisationen und ausgewählte Staaten.

2.3 Verwaltungsvereinbarung zu NEDIK

Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) hat in der Herbstversammlung vom 12. November 2020 eine Verwaltungsvereinbarung mit der Konferenz der Kantonalen Polizeikommandanten (KKPKS) gutgeheissen, welche die Organisation und die Finanzierung des Netzwerks digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) regelt.[3] Die Vereinbarung trat am 1. Januar 2021 in Kraft.
Die KKPKS hat NEDIK bereits im Jahr 2018 gegründet, mit dem Ziel, die Spezialressourcen zu bündeln und damit die digitale Kriminalität effizient zu bekämpfen. Mit der Verwaltungsvereinbarung wurden die Organisation und Finanzierung von NEDIK geregelt.
NEDIK ist als Netzwerk unter anderem für die Sicherstellung des gegenseitigen Wissenstransfers, für die Erstellung einer nationalen Fallübersicht sowie die Triage von interkantonalen Fällen verantwortlich. Ausserdem leistet NEDIK einen Beitrag an die Prävention und arbeitet mit der Schweizerischen Kriminalprävention (SKP) und mit dem Nationalen Zentrum für Cybersicherheit (NCSC) zusammen.
Innerhalb von NEDIK übernimmt fedpol die überkantonale und transnationale Koordination, insbesondere bei der Zusammenarbeit mit Partnerbehörden im Ausland. fedpol erstellt Analyseberichte und vertritt die Schweiz in internationalen Expertengruppen.

[2] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-83160.html

[3] https://www.kkjpd.ch/newsreader/verst%C3%A4rkter-einsatz-der-kantone-gegen-cyber-und-p%C3%A4dokriminalit%C3%A4t.html

2.4 Strategie Digitalaussenpolitik

Im November 2020 hat der Bundesrat die Strategie Digitalaussenpolitik verabschiedet.[4] Die Strategie hält zum Thema Cybersicherheit fest, dass die Schweiz die Friedensförderung überall wo dies möglich ist, verstärken will. Beim digitalen Raum gilt es konkret, Strukturen und Dialogforen zu stärken, die zur Einhaltung des Völkerrechts einschliesslich des humanitären Völkerrechts beitragen. Die Schweiz bekennt sich zu den geltenden völkerrechtlichen Normen und setzt sich dafür ein, dass diese im Kampf gegen sämtliche Formen von Cyberangriffen zur Anwendung kommen. Cybersicherheit betrifft sämtliche Akteure – von Regierungen über privatwirtschaftliche Akteure bis hin zur Zivilgesellschaft. Bei der strategischen Ausrichtung der Schweizer Aussenpolitik ist der Multistakeholder-Ansatz ein Kernelement, genauso wie die lange Tradition der guten Dienste.

[4] https://www.eda.admin.ch/dam/eda/de/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_DE.pdf

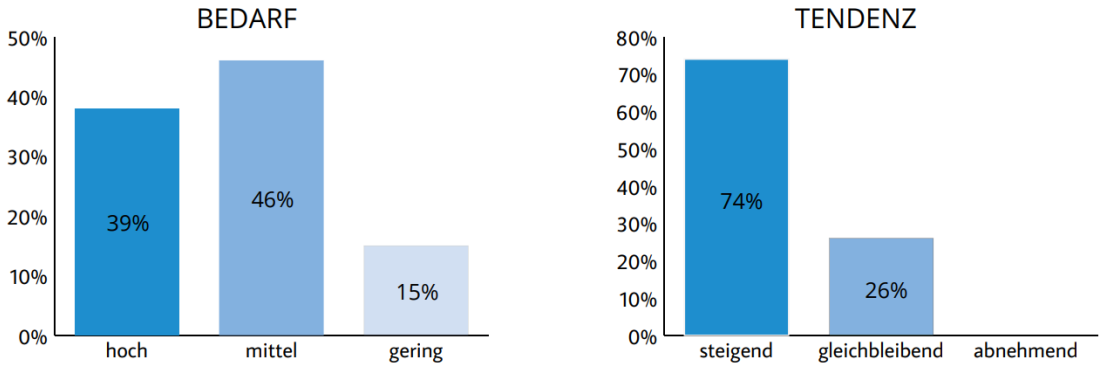
3 Inhaltliche Schwerpunkte der Umsetzung der NCS

Parallel zur weiteren Etablierung der Cyberorganisation des Bundes laufen die Umsetzungsarbeiten zur NCS. Diese wird nicht durch die Bundesverwaltung alleine vorangetrieben, sondern wesentlich durch Akteure der Kantone, der Wirtschaft, den Hochschulen und der Wirtschaft mitgetragen. Während in Kapitel 5 die erreichten Meilensteine in allen Handlungsfeldern kurz beschrieben werden, soll im vorliegenden Kapitel auf Schlüsselprojekte der aktuell laufenden Arbeiten eingegangen werden.

3.1 Aufbau des Nationalen Testinstituts für Cybersicherheit (NTC)

Die Sicherheit digitaler Produkte ist für die Cybersicherheit von entscheidender Bedeutung. Enthalten die Produkte Sicherheitslücken, besteht insbesondere bei einer Anwendung dieser Produkte durch kritische Infrastrukturen eine reale Bedrohung mit erheblichem Schadenspotential für Wirtschaft und Gesellschaft. Bisher gibt es in der Schweiz aber nicht genügend Kapazitäten zur Prüfung solcher Produkte auf mögliche Sicherheitslücken.
Auf Initiative des Kantons Zug wurde deshalb das «Nationale Testinstitut für Cybersicherheit» (NTC) lanciert. Im Rahmen dieses Vorhabens wurde im Oktober 2020 bei Betreiberinnen kritischer Infrastrukturen eine Befragung durchgeführt, um zu klären, ob ein Bedarf für ein Testinstitut besteht. Die Resultate waren eindeutig: Bei rund 85 % der teilnehmenden Organisationen besteht sowohl der Bedarf für Prüfungen der Cybersicherheit als auch die Bereitschaft diese Aufträge an das NTC zu übergeben. 75 % der teilnehmenden Organisationen vermuten, dass der Prüfbedarf in den nächsten Jahren noch weiter zunimmt. Dass er abnimmt, vermutet hingegen niemand.

«Wie gross schätzen Sie den Bedarf für Prüfungen der Cybersicherheit in Ihrer Organisation in den nächsten 5 Jahren ein, den Sie an ein nationales Testinstitut für Cybersicherheit übergeben würden?»
N=64



Im November 2020 wurde daraufhin der Verein «Nationales Testinstitut für Cybersicherheit NTC» gegründet. Der Verein ist Projekttreiber und nach Abschluss des Projektes der Träger des Betriebs. Der Bund hat die Initiative bisher fachlich begleitet. In einem Parlamentarischen Vorstoss forderte Nationalrat Franz Grüter im Dezember 2020 eine Beteiligung des Bundes beim Aufbau und Betrieb des NTC (20.4495).
Seit 2021 führt das NTC nun erste Pilot-Prüfprozesse durch, entwickelt das Businessmodel und definiert die Trägerschaft des NTC für die eigentliche Operationalisierung.

3.2 Label cyber-safe.ch für Schweizer Gemeinden

Die Informationstechnologie spielt heute in den Gemeinden eine zentrale Rolle, von der Verwaltung von Kläranlagen, über kommunale Heizsysteme, bis hin zum E-Government. Daher können Gemeinden, unabhängig von ihrer Grösse und ihren Mitteln, das Thema Cybersicherheit nicht länger ignorieren. Deshalb wird seit Mitte 2020 in einem Pilotprojekt mit Unterstützung der NCS, dem Schweizerischen Sicherheitsverbund (SVS) und des Schweizerischen Gemeindeverbandes (SGV) die Cybersicherheit von rund fünfzehn Schweizer Gemeinden mit Hilfe des Labels «cyber-safe.ch» getestet, um sie über die zu treffenden Massnahmen zu informieren und ihnen gegebenenfalls das Label zu verleihen - nach dem Beispiel der Gemeinde Bussigny (VD) oder Jonen (AG).
Das Pilotprojekt soll dem NCSC ermöglichen, den Nutzen eines Gütesiegels für Cybersicherheit für Gemeinden und öffentliche Verwaltungen zu evaluieren und Lehren für künftige Massnahmen zu ziehen.

3.3 Label für IT-Dienstleister

Mit der voranschreitenden Digitalisierung sind Kleine und mittlere Unternehmen (KMU) zunehmend der Bedrohung aus dem Cyberraum ausgesetzt. Gleichzeitig greifen Schweizer KMU immer öfter auf externe IT-Dienstleister zurück: Heute arbeiten zwei Drittel der KMU mit IT-Dienstleistern zusammen. Weil IT-Dienstleister einen direkten Einfluss auf die Cyberresilienz der KMU haben, ist es zwingend notwendig, dass sie grundlegende technische und organisatorische Kompetenzen in IT- und Informationssicherheit mitbringen.
Eine öffentlich-private Trägerschaft, bestehend aus Partnern von Bund und Akteuren aus der Privatwirtschaft, hat im 4. Quartal 2020 die Initiative zur Schaffung eines unabhängigen Gütesiegels für IT-Dienstleister ins Leben gerufen. Das Gütesiegel zeichnet IT-Dienstleister aus, die ihren Kunden mit den nötigen technischen und organisatorischen Massnahmen ein angemessenes Schutzniveau gewährleisten. Die Erlangung des Gütesiegels beeinflusst somit die Cyberresilienz der KMU positiv, verankert die Digitalisierung auf einem höheren Qualitätsniveau und stärkt somit das Vertrauen in die digitale Sicherheit der Schweiz
Das Konzept des Gütesiegels wurde im Dezember 2020 definiert und erstellt. Von Januar 2021 bis März 2021 folgte eine Pilotierung mit vier IT-Dienstleistern. Von Mai bis Juli 2021 wurde eine erweiterte Testphase mit zehn IT-Dienstleistern durchgeführt. Parallel dazu wurde im Mai 2021 mit der Erarbeitung des Go-to-Market Konzepts (u.a. Website, Kommunikation, Marketingmassnahmen, Aufbau Auditor*innennetzwerk, Geschäfts- und Betriebsprozess) gestartet. Der Markteintritt mit der Überführung in die Betriebsphase durch den neu gegründeten Verein ist im September 2021 geplant.

3.4 Nationale Sensibilisierungskampagne

In der Woche vom 3. bis zum 7. Mai 2021 fand die erste nationale Sensibilisierungskampagne zur Cybersicherheit in Form einer Aktionswoche statt. Die Kampagne wurde unter der Trägerschaft von NCSC, der Schweizerischen Kriminalprävention (SKP), Hochschule Luzern (HSLU) und der SISA (Swiss Internet Alliance)/iBarry durchgeführt. Verschiedene Partner haben die Trägerschaft zudem unterstützt, indem sie die Kampagne über ihre Kanäle verbreitet haben. Darunter waren Digitalswitzerland, Digital Liechtenstein, die Mitglieder der SISA wie bspw. Swisscom, UPC-Sunrise, SWITCH, die Mobiliar sowie knapp 100 Banken als Ansprechpartner von «eBanking – aber sicher!» und alle kantonalen und städtischen Polizeikorps.
Während fünf Tagen wurde an jedem Tag ein Thema vorgestellt, das die Bürgerinnen und

Bürger einerseits sensibilisieren und ihnen andererseits Hilfsmittel zum eigenverantwortlichen Handeln im digitalen Raum mitgeben sollte. Die Themen umfassten: Datensicherung, Passwörter, Updates, Virenschutz und Achtsamkeit. Die Inhalte wurden vornehmlich online und insbesondere auf Social Media vermittelt und gestreut.

3.5 Pilotversucht mit «Bug Bounty Switzerland»

Das NCSC hat sich entschieden, gemeinsam mit der Firma «Bug Bounty Switzerland» einen Pilotversuch zu starten, in welchem ethische Hacker beauftragt werden, Schwachstellen in Systemen der Bundesverwaltung zu suchen. Finden sie solche, erhalten sie eine der Bedeutung der gefundenen Schwachstelle angemessene finanzielle Belohnung.
Der Pilotversuch startete am 10. Mai 2021 und dauerte elf Tage. 15 Hacker haben insgesamt sechs IT-Systeme des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) und der Parlamentsdienste getestet. Sie haben dabei zehn Schwachstellen gefunden. Diese Zahl ist für einen erstmaligen Test mit ethischen Hackern im Vergleich tief und zeigt auf, dass sämtliche der getesteten IT-Systeme über eine hohe Sicherheitsmaturität verfügen und kein leichtes Ziel darstellten. Trotzdem gibt es auch in solchen Umgebungen Schwachstellen, die trotz aller bestehenden Sicherheitsmassahmen in den öffentlich im Internet stehenden Systemen noch vorhanden sind und die Notwendigkeit eines Bug Bounty Programms deutlich aufzeigen. Das NCSC will auf Grund der gemachten Erfahrungen weiterhin Bug Bounty Programme für die Bundesverwaltung anwenden.[5]

3.6 Erarbeitung einer Vernehmlassungsvorlage zur Meldepflicht für Cyberangriffe

Der Bundesrat hat das EFD (NCSC) am 11. Dezember 2020 damit beauftragt, in Zusammenarbeit mit den betroffenen Stellen aller Departemente bis Ende 2021 eine Vernehmlassungsvorlage zu erarbeiten, welche Meldepflichten bei Cyberangriffen für Betreiberinnen kritischer Infrastrukturen einführt. Es soll dazu eine zentrale Meldestelle bestimmt werden, welche die Meldungen zur Verbesserung der Frühwarnung vor Cybergefahren nutzt und statistische Daten zu Cybervorfällen erfasst. Die neue Meldepflicht soll auf bereits bestehende Meldepflichten (insbesondere die datenschutzrechtliche Meldepflichten) abgestimmt werden.
Das NCSC hat im April 2021 unter Betreiberinnen kritischer Infrastrukturen und Behörden eine Umfrage zur Meldepflicht für Cybervorfälle durchgeführt. Diese hat ergeben, dass die Akzeptanz gegenüber einer Meldepflicht grundsätzlich hoch ist, wenn es gelingt, diese so umzusetzen, dass ein geringer bürokratischer Aufwand entsteht. Abbildung 2 zeigt, wie die Akzeptanz der Meldepflicht bei den Befragten (N=400) verteilt ist, wobei die Skala von 1 «mit der Einführung der Meldepflicht bin ich überhaupt nicht einverstanden» bis 5 «mit der Einführung der Meldepflicht bin ich voll und ganz einverstanden» reicht. Die Erkenntnisse der durchgeführten Umfrage werden genutzt, um die Vernehmlassungsvorlage im weiteren Verlaufe des Jahres 2021 auszugestalten.

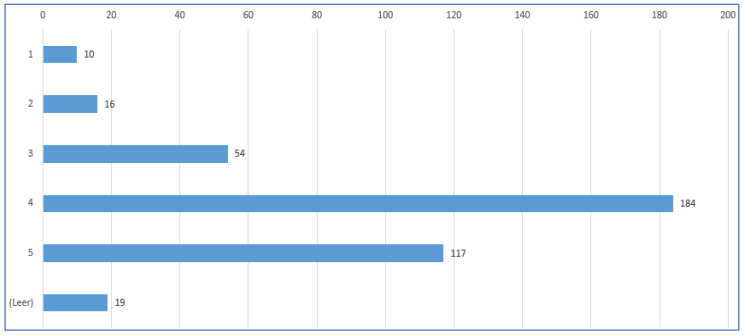


Abbildung 2: Akzeptanz der Meldepflicht

[5] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-84304.html

4 Detaillierter Umsetzungsstand

In diesem Kapitel wird der Stand der Umsetzung der NCS auf Grund der Meilensteinplanung aufgezeigt. Für jede Massnahme wird aufgezeigt, welche Meilensteine bis im zweiten Quartal 2021 erreicht oder nicht erreicht wurden. Zudem werden die Meilensteine kurz beschrieben, damit klar ist, um welchen Beitrag es sich handelt.
Insgesamt wurden von den 275 im Umsetzungsplan der NCS definierten Meilensteine 154 umgesetzt, 8 wurden bislang nicht erreicht. 6 von 29 Massnahmen sind damit vollständig abgeschlossen. Mit einem Umsetzungsstand von nicht ganz zwei Dritteln nach 14 von total 20 Quartalen Laufzeit der NCS lässt sich feststellen, dass die Umsetzung der NCS generell nach wie vor auf Kurs ist, sodass die ausstehenden Arbeiten in den verbleibenden Quartalen wie geplant umgesetzt werden können. Abbildung 3 verdeutlicht den Umsetzungsstand über alle Meilensteine hinweg.

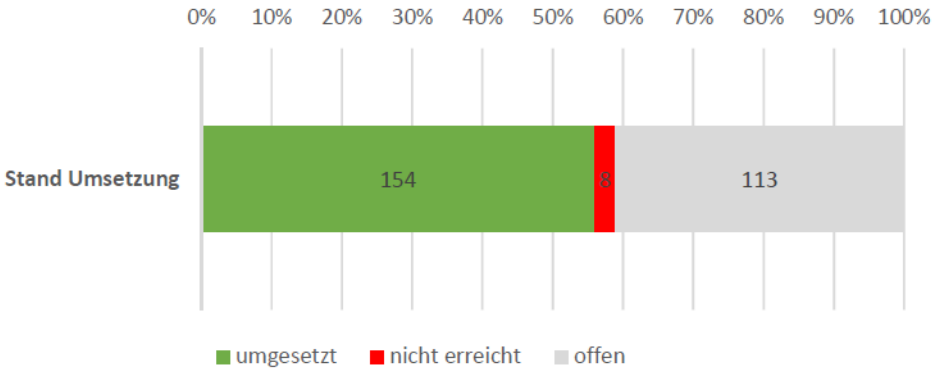


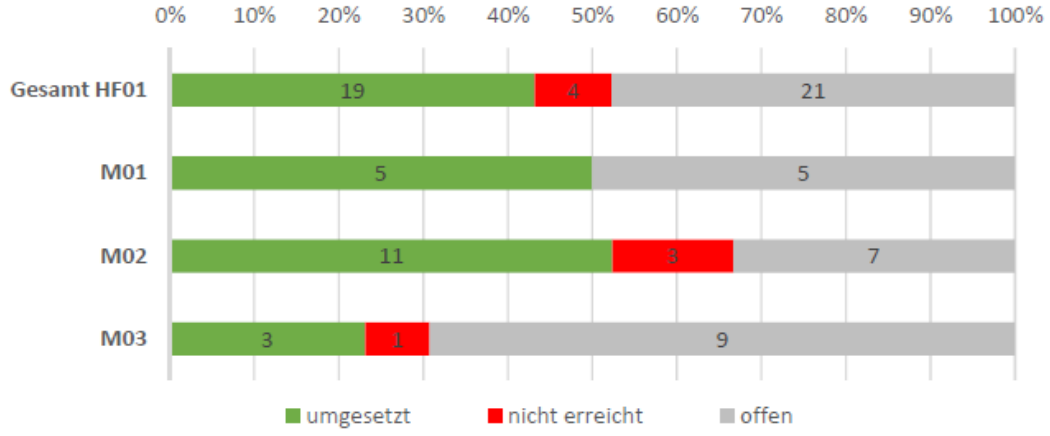
Abbildung 3 Umsetzungsstand der NCS-Meilensteine

4.1 Handlungsfeld 1 «Kompetenzen- und Wissensaufbau»

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M1 Früherkennung von Trends und Technologien und Wissensaufbau (armasuisse W+T)
- M2 Ausbau und Förderung von Forschungs- und Bildungskompetenz (NCSC und armasuisse W+T)
- M3 Schaffung von günstigen Rahmenbedingungen für eine innovative IKT-Sicherheitswirtschaft in der Schweiz (NCSC)

Status der Umsetzung:



Meilensteine 2018 – Q2 2021

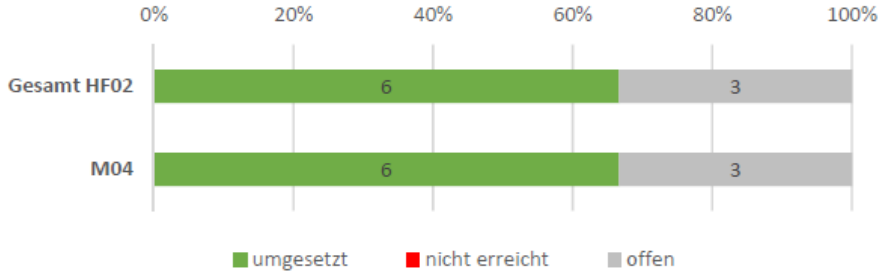
	Meilensteine	Status
M1	Technologiemonitoring: 1) Leistungen des CYD Campus für das Monitoring zuhanden des NCSC sind festgelegt 2) Aufnahme des Betriebs des Monitorings 3) Erste Auswertung zu Monitoring liegt vor	umgesetzt
	Trendanalyse: 1) Konzept für Zielpublikum, Inhalte, Verbreitung der Berichte ist erstellt 2) Aufträge für Auswertung sind erteilt	umgesetzt
M2	Bedarfsanalyse zu Bildungsangebote: 1) Übersicht der bestehenden Bildungsangebote ist erstellt 2) Analyse erstellt und Zielgruppen sind definiert	umgesetzt *«Vorhaben vorzeitig abgeschlossen: Angebotsübersicht zeigt, dass sich Markt mittlerweile etabliert hat.»*
	Forschungs- und Supportzentrum der beiden ETH: 1) Konzept für das Forschungs- und Supportzentrum ist erstellt 2) Fragen der Finanzierung und Lokalität sind geklärt 3) Forschungszentrum nimmt Betrieb auf, mit schrittweisen Ausbau in der Jahren 2021-2022	umgesetzt
	Cyber Defence Campus: 1) Standort Thun nimmt Betrieb auf 2) Standort EPFL nimmt Betrieb auf 3) Standort ETHZ nimmt Betrieb auf	umgesetzt
	Interdisziplinäre Forschung und Bildung zur Cybersicherheit: 1) Wichtigste Forschungsinstitute im Bereich Cyberrisiken sind identifiziert	umgesetzt
	Förderung «Ethical Hacking»: 1) Etablierte Anlässe im Bereich «Ethical Hacking» sind identifiziert 2) Förderinstrumente sind ausgestaltet; Finanzmittel, wenn nötig beantragt	umgesetzt Vorhaben sistiert: *Finanzierung durch Bund ist nicht das geeignete Mittel, Anlässe im Bereich Ethical Hacking zu fördern. Mittel in Bug Bounty investiert.*
	Durchführung Pilot Bug Bounty Programm: 1) Vertrag zw. Bug Bounty Switzerland und NCSC liegt vor 2) Pilotprojekt durchgeführt und Auswertung und Erfahrungsbericht liegt vor	umgesetzt
M3	Aufbau von Innovations-Zentren: 1) Vorschlag für Aufbau und Finanzierung eines nationalen Cyber-Hubs ist erarbeitet	Vorhaben sistiert: *Aufgrund von bestehenden Initiativen (wie trust valley, Zuger Initiative usw.) sowie Erfahrungen aus Gesprächen v.a. mit den Kantonen. Vorhaben wird im Umsetzungsplan sistiert und ggf. im Rahmen der neuen NCS-Strategie neu evaluiert.*
	Think Tank: 1) Konzept für das Forschungs- und Supportzentrum der beiden ETH ist erstellt 2) Fragen der Finanzierung und Lokalität für das Forschungs- und Supportzentrum der beiden ETH sind geklärt 3) Forschungszentrum mit Think Tank nimmt Betrieb auf, mit schrittweisen Ausbau in der Jahren 2021-2022	umgesetzt

4.2 Handlungsfeld 2 «Bedrohungslage»

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M4 Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyberbedrohungslage (NDB)

Status der Umsetzung:



Meilensteine 2018 – Q2 2021

	Meilensteine	Status
M4	Identifikation der Zielgruppen und ihrer Bedürfnisse: 1) Identifikation erweiterter Zielgruppen und deren Bedürfnisse liegen vor 2) Kommunikationskanäle für die jeweiligen Zielgruppen identifiziert	umgesetzt
	Definition Produktekatalog pro Zielgruppe (Leistungskatalog): 1) Aufgabenbereich zw. Bund und Wirtschaft geklärt 2) Leistungskatalog per Zielgruppe definiert	umgesetzt
	Aufbau benötigter Quellen und Produktionsressourcen: 1) Liste zusätzlich benötigter Quellen erstellt 2) Projekt zum Aufbau der technischen Unterstützung vorhanden	umgesetzt

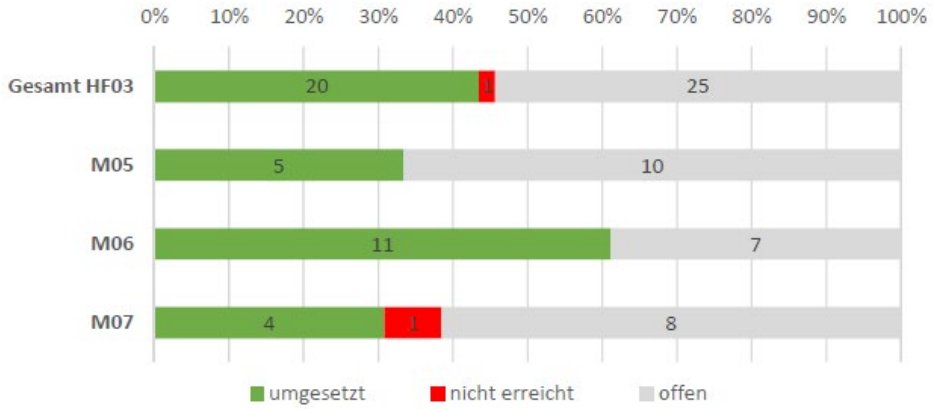
4.3 Handlungsfeld 3 «Resilienz-Management»

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M5 Verbesserung der IKT-Resilienz der kritischen Infrastrukturen (BABS in Zusammenarbeit mit den Fachämtern in regulierten Sektoren)
- M6 Verbesserung der IKT-Resilienz der Bundesverwaltung (NCSC)
- M7 Erfahrungsaustausch und Schaffung von Grundlagen zur Verbesserung der IKT-Resilienz in den Kantonen (NCSC, SVS)[6]

[6] Informationen zu weiteren Projekten des Umsetzungsplans der Kantone zur NCS 2018–2022 vom SVS und deren Umsetzungsstand finden Sie hier: https://www.svs.admin.ch/de/themen-/cybersicherheit/cybersicherheit-kantone.html#441_1612790888827

Status der Umsetzung:



Meilensteine 2018 – Q2 2021

	Meilensteine	Status
M5	Umsetzung der geplanten bzw. laufenden Projekte zur Stärkung der Resilienz in den kritischen Teilsektoren: 1) Bestandsaufnahme der umgesetzten und noch nicht umgesetzten Vorhaben aus den Massnahmenberichten erstellt 2) Verantwortlichkeiten für die Umsetzung sind geklärt 3) Roadmap/Planung der laufenden und anstehenden Massnahmen erarbeitet	umgesetzt
	Etablierung einer akademischen Arbeitsgruppe für Cybersicherheit: 1) Bestandsaufnahme von Projekten und aktiven Gruppen 2) Institutionalisieren der Arbeitsgruppe	umgesetzt
M6	Sicherheitsvorgaben für agile Projektmethoden entwickeln: 1) Bestehenden sicherheitsrelevanten Aufgaben und Ergebnisse in Projektmethoden analysiert 2) Zusätzliche Aufgaben und Ergebnisse sowie Ergänzungen bestehender Teile identifiziert und beschrieben	umgesetzt
	Sensibilisierungskampagne in der Bundesverwaltung: 1) Grobkonzept Sensibilisierungskampagne IKT-Sicherheit in der Bundesverwaltung «SIB 19» erstellt (Q4/2018) 2) Start der Sensibilisierungskampagne IKT-Sicherheit in der Bundesverwaltung «SIB» 3) Abstimmung mit aktiven Akteuren zur konzeptionellen Ausdehnung zu einer nationalen Kampagne durchgeführt	umgesetzt
	Sichere Datenübertragung (SCION): 1) Absichtserklärung interessierter Bedarfsträger und Pilotanwendern 2) Aufbau und Inbetriebnahme der Pilotanwendungen umgesetzt	umgesetzt
	Security Operations Center (SOC) BIT: 1) Konzept und Umsetzungsplan	umgesetzt
	Schaffung einer Schnittstelle zum ETH-Bereich: 1) Koordination mit dem Delegierten des Bundes für Cybersicherheit 2) Durchführung konkreter Massnahmen 3) Gemeinsame Koordination	umgesetzt
M7	Permanenter Austausch Kantone: 1) Anforderungsklärung der Arbeitsplatzausstattung bei NCSC	Vorhaben sistiert: *Aussetzung des Vorhabens v.a. aufgrund der Pandemie mit Neubeurteilung auf anfangs 2022 unter Berücksichtigung der NCSC-Ausrichtung.*
	Durchführung der Cyber-Landsgemeinde: 1) Durchführung Landsgemeinde 2019	umgesetzt

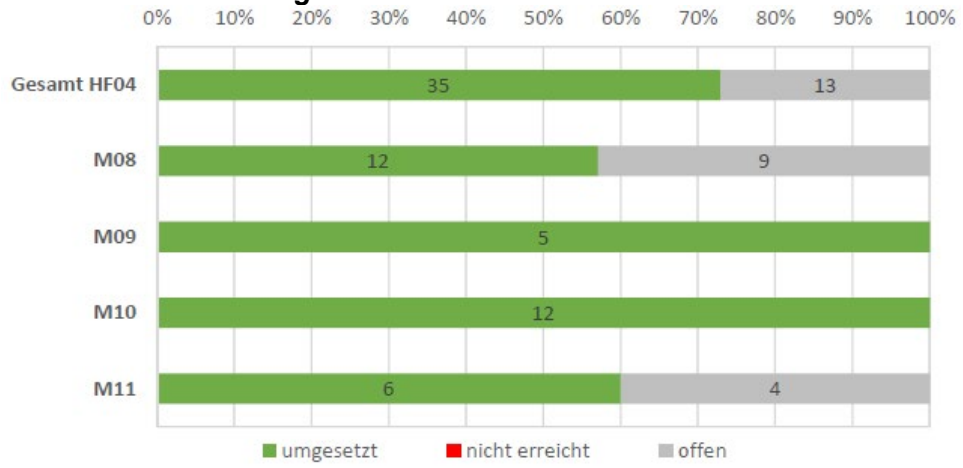
	2) Durchführung Landsgemeinde 2020	
	Schaffung Schnittstelle ETH zu Kantonen: 1) Koordination mit dem SVS 2) Durchführung konkreter Massnahmen	umgesetzt

4.4 Handlungsfeld 4 «Standardisierung / Regulierung»

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M8 Evaluierung und Einführung von Minimalstandards (BWL)
- M9 Prüfung einer Meldepflicht für Cybervorfälle und Entscheid über Einführung
- M10 Globale Internet-Gouvernanz (BAKOM)
- M11 Aufbau von Expertise zu Fragen der Standardisierung in Bezug auf Cybersicherheit (NCSC)

Status der Umsetzung:



Meilensteine 2018 – Q2 2021

	Meilensteine	Status
M8	Entwicklung und Umsetzung von Minimalstandards für die IKT-Resilienz: 1) Publikation des IKT-Minimalstandards und Hilfsmittel für das Assessment 2) Minimalstandard «Handbuch Grundschutz» des Verbands Schweiz. Elektrizitätsunternehmen (VSE) 3) Branchenstandards zu Trinkwasser, Lebensmittel, Erdgas und Öffentlicher Verkehr	umgesetzt
	Entwicklung und Etablierung von Hilfsmittel für KMU: 1) Publikation Cybersecurity-Schnelltest für KMU (SATW) [Q3/2018] 2) Bedarfsanalyse zu weiteren Hilfsmittel (technische Hilfsmittel, Labels, Leitfäden, Anleitungen) für KMU 3) Prüfung möglicher Einführung von Labels und Normen ist abgeschlossen	umgesetzt
	Label Cyber-Safe für Gemeinden: 1) Vertrag zw. Cyber-Safe und NCSC und Vereinbarung zw. NCSC und dem Schweizerischen Gemeindeverband visiert 2) Projekt-Roadmap erstellt und die Vereinbarungen zu den 15 Pilotgemeinden liegen vor	umgesetzt
	Label für IT-Dienstleister: 1) Vertrag zw. Digitalswitzerland und NCSC unterschrieben 2) Erarbeitung der Grundlagen für das Label (Prüfhandbuch, Kontrollliste usw.)	umgesetzt
M9	Studie über Grundmodelle von Meldepflichten: 1) Ausschreibung und Verfassen einer Grundstudie 2) Berichterstattung über die Grundmodelle sowie Empfehlungen hierzu	umgesetzt
	Grundsatzdiskussion mit Wirtschaft und Behörden: 1) Weiterführende Diskussion mit Wirtschaft und Politik	umgesetzt

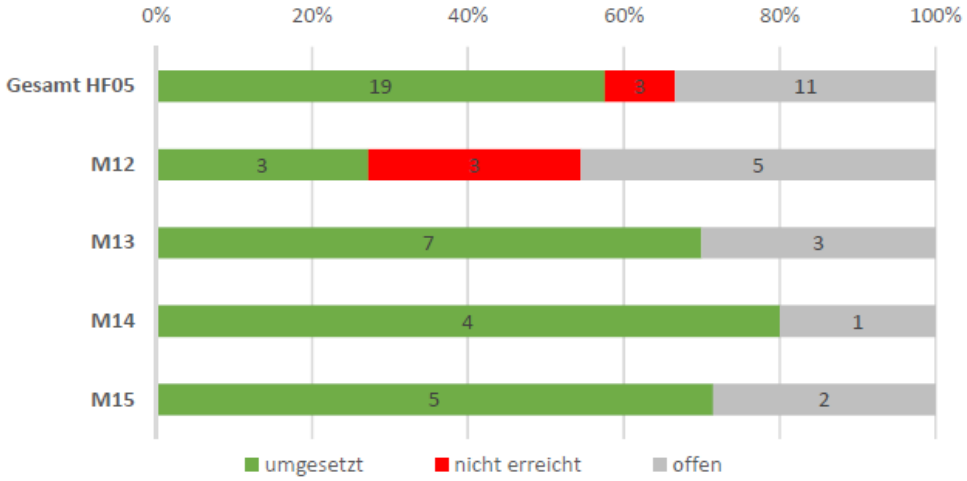
	2) Grundlage für Entscheid zur Meldepflicht	
M10	Treffen des hochrangigen Panels des UN-Generalsekretärs: 1) Treffen in New York, Genf und Helsinki 2) Abschlussbericht des Panels 3) Evaluation Umsetzungsmöglichkeiten des Berichts	umgesetzt
	Multistakeholder-Austauschplattformen zur Koordination auf nationaler Ebene: 1) Swiss-IGF 2018 (Q4/2018) 2) Swiss-IGF 2020	umgesetzt
M11	Schaffung eines überdepartementalen Expertenpool Cyber: 1) Bedarfsabklärung 2) Konzeption des Expertenpools und Beschluss der Ressourcen	umgesetzt
	Stärkung von Standardisierungsvorhaben durch die Unterstützung der Hochschulen: 1) Konzept der Gemeinsamen Forschungs- und Unterstützungsstelle EPFL-ETHZ erstellt 2) Überblick über die Aktivitäten der Schweiz in diesem Bereich erstellt 3) Umsetzung der Aktivitäten in den als strategisch identifizierten Arbeitsgruppen	umgesetzt
	Beitrag der Schweiz zur Verankerung des Themas Cybersicherheit in der internationalen Finanzpolitik: 1) Erster Zwischenbericht zu den Aktivitäten zur Stärkung der internationalen Cyberkapazitäten in der Finanzwirtschaft	umgesetzt

4.5 Handlungsfeld 5 «Vorfallbewältigung»

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M12 Ausbau von MELANI als Public-Private-Partnership für die Betreiberinnen kritischer Infrastrukturen (NCSC)
- M13 Aufbau von Dienstleistungen für alle Unternehmen (NCSC)
- M14 Zusammenarbeit des Bundes mit relevanten Stellen und Kompetenzzentren (NCSC)
- M15 Prozesse und Grundlagen der Vorfallbewältigung des Bundes (NCSC)

Status der Umsetzung:



Meilensteine 2018 – Q2 2021

	Meilensteine	Status
M12	Gezielte Erweiterung des geschlossenen Kundenkreises: 1) Situationsanalyse über Nutzung von MELANI durch die verschiedenen kritischen Sektoren ist erstellt	verzögert: *Aufgrund der strategischen Weiterentwicklung verschoben, mit Neubeurteilung und Neuplanung auf anfangs 2022*
	Entwicklung und Erweiterung von Dienstleistungen und Produkten: 1) Analyse der bestehenden MELANI Produkte und Dienstleistung sowie des bestehenden Bedarfs	umgesetzt
	Ausbau der bestehenden Austauschplattform 1) Studie mit Variantenempfehlung zu MELANI-NET 2.0 erstellt (Q3/2018) 2) PoC (Proof of Concept) zur empfohlenen Variante durchgeführt 3) Konzept MELANI-NET 2.0 4) und MELANI-NET 2.0 produktiv	umgesetzt umgesetzt verzögert: *Aufgrund der strategischen Weiterentwicklung der Informationsplattformen der NCSC verschoben, mit Neubeurteilung und Neuplanung auf anfangs 2022*
M13	Schaffung einer nationalen Anlaufstelle Cyber: 1) Grobkonzept für das Online-Portal für die Meldung von Cybervorfällen erstellt 2) Online-Portal für die Meldungen von Cyber-Vorfällen steht der Öffentlichkeit zur Verfügung 3) Integration in die Informationsplattform zu Cyber-Risiken ist erfolgt (vgl. M29)	umgesetzt
	Zeitnahe Information im Ereignisfall über die Alertswiss-App: 1) Anforderungsklärung bezüglich Alarmierung, Warnung und Information der Öffentlichkeit im Cyber-Vorfall zwischen Kompetenzzentrum und BABS ist erfolgt 2) Konzept zur Integration der Cyber-Informationen im Alertswiss-App ist erstellt 3) Information der Öffentlichkeit im Cyber-Ereignis über Alertswiss-App ist möglich 4) Information über die Neuerung (Cyber-Ereignis) im Alertswiss-App publiziert	umgesetzt
M14	Übersicht über bestehende operative SOCs und CERTs inkl. Ansprechpartner: 1) Erhebung der bestehenden operativen SOCs und CERTs inklusive Ansprechpartner durchgeführt und dokumentiert 2) Prozess sowie Verantwortung zur laufenden Aktualisierung der Übersicht geklärt	umgesetzt
	Informationsaustausch mit CERTs und SOCs: 1) Analyse zum Bedarf und den Möglichkeiten eines systematischen Informationsaustausches 2) Projekte für die Etablierung des Informationsaustausches sind definiert und zugewiesen	umgesetzt
M15	Erarbeitung Cyberverordnung zur Cybersicherheit: 1) Erarbeitung der Verordnung 2) Beschluss der Verordnung durch Bundesrat 3) Inkrafttreten der Verordnung festgelegt	umgesetzt
	Erstellung eines Sicherheitsvorfallbewältigungsprozesses für die Bundesverwaltung: 1) Erster Entwurf für einen Prozess, Diskussion mit Leistungserbringern und betroffenen Stellen (Q3/2018)	umgesetzt

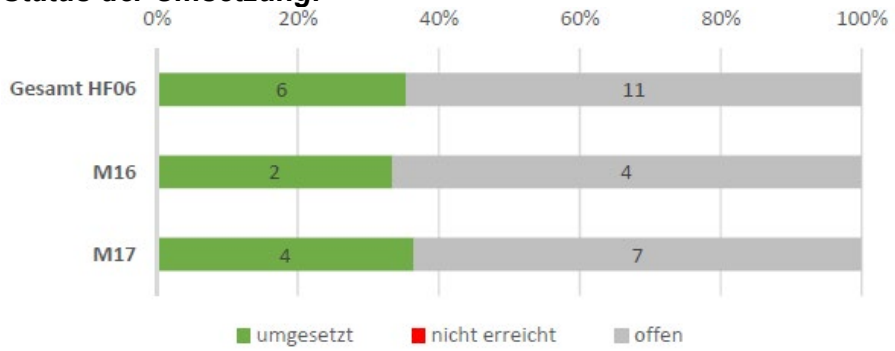
	2) Prozess ist auf die Verordnung Cybersicherheit angepasst	

4.6 Handlungsfeld 6 «Krisenmanagement»

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M16 Integration der zuständigen Fachstellen aus dem Bereich Cyber-Sicherheit in die Krisenstäbe des Bundes (NCSC)
- M17 Gemeinsame Übungen zum Krisenmanagement (NCSC, GS VBS)

Status der Umsetzung:



Meilensteine 2018 – Q2 2021

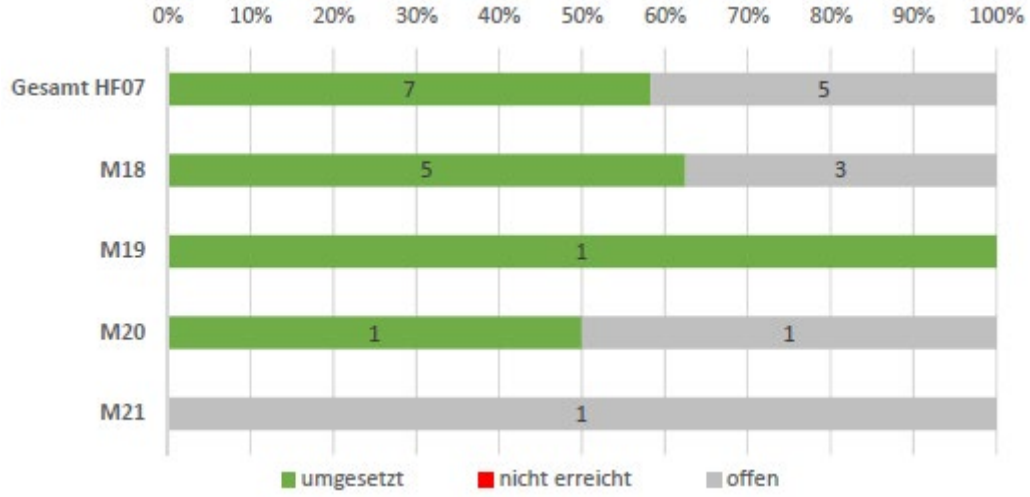
	Meilensteine	Status
M16	Erweiterung Cyber Glossar: 1) Bestandsaufnahme der vorhandenen Definitionen 2) Cyber-Glossar über-/erarbeitet	umgesetzt
M17	Schaffung von Grundlagen für Krisenübungen mit Cyberaspekten: 1) Bestandaufnahme bestehender und geplanten nationaler und internationaler Krisenübungen mit Cyberaspekten 2) Prozess zur Aktualisierung und Abstimmung zur Cyberübungsübersicht	umgesetzt
	Durchführung von sektorspezifischen Übungen: 1) Bedarfsanalyse zu sektorspezifischen Krisenübungen ist erfolgt	umgesetzt
	Einbringen von Cyber-Aspekten in übergreifende Krisen-übungen: 1) Abstimmung mit den verantwortlichen Übungspartnern zum Einbezug der relevanten Cyber-Kriterien in der Übung durchgeführt	umgesetzt

4.7 Handlungsfeld 7 «Strafverfolgung»

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M18 Fallübersicht Cyber-Kriminalität (fedpol und KKPKS mit NEDIK)
- M19 Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (fedpol als Teil der KKPKS)
- M20 Ausbildung (KKPKS [inkl. fedpol], SSK [inkl. BA])
- M21 Zentralstelle Cyber-Kriminalität (fedpol)

Status der Umsetzung:



Meilensteine 2018 – Q2 2021

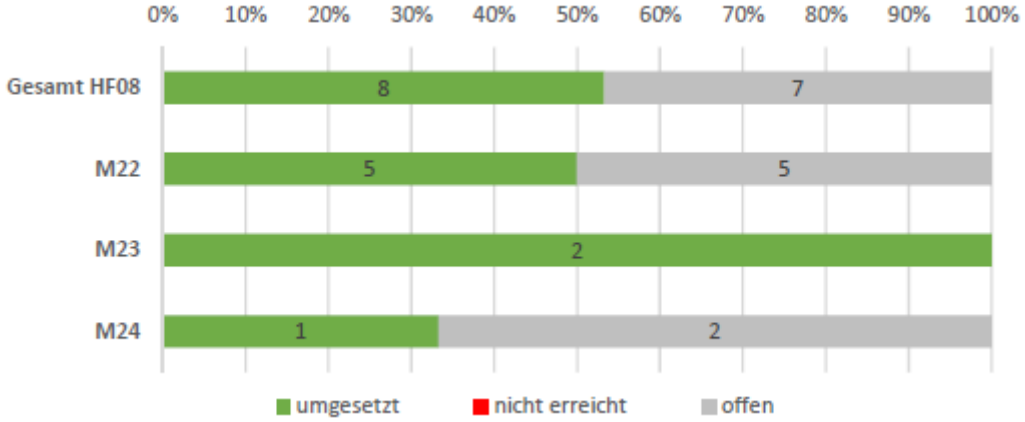
	Meilensteine	Status
M18	Fallübersicht Cyber-Kriminalität (PICSEL): 1) Testphase PICSEL gestartet	umgesetzt
	Erarbeitung einer justiziellen Fallübersicht: 1) Tool Cyber-CASE; Fallkomplex-Liste sämtlicher Cyber-SPoC-StA (bereits operativ) 2) Online Tool für die Verfahrensübersicht der laufenden Verfahren	umgesetzt
	Aufzeigen von Entwicklungen, Szenarien und Auswirkungen: 1) Monatliches Bulletin (polizeilich) NEDIK 2) Übersicht der laufenden Verfahren (polizeilich & justiziell)	umgesetzt
M19	Rechtlichen Grundlagen für die Zusammenarbeit und Verrechnung von Leistungen zw. Bund und Kantonen und unter Kantonen: 1) Vereinbarung(en) unterzeichnet und verabschiedet	umgesetzt
M20	Umsetzung der Ausbildungskonzepte: 1) Übersicht der Akad. Ausbildungsmöglichkeiten (polizeilich)	umgesetzt
M21	Keine Meilensteine bis Q2 2021	

4.8 Handlungsfeld 8 «Cyberdefence»

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M22 Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution (NDB)
- M23 Fähigkeit zur Durchführung von aktiven Massnahmen im Cyber-Raum gemäss NDG und MG (NDB, FUB-ZEO)
- M24 Gewährleistung Einsatzbereitschaft der Armee über alle Lagen im Cyber-Raum und Regelung ihrer subsidiären Rolle zur Unterstützung der zivilen Behörden (GS VBS und FUB)

Status der Umsetzung:



Meilensteine 2018 – Q2 2021

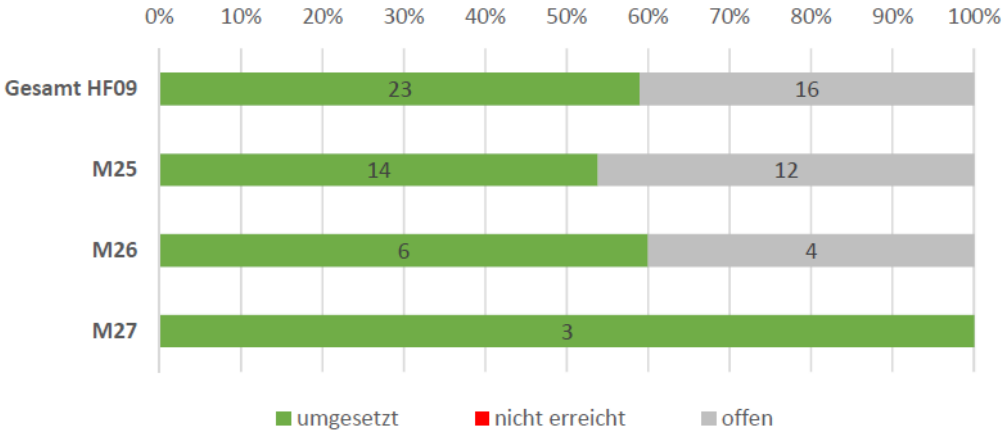
	Meilensteine	Status
M22	Fähigkeiten zur Informationsbeschaffung und Attribution: 1) Ausbau erste Etappe ist erfolgt	umgesetzt
	Durchführung einer spezifischen Ausbildung in der Cyberabwehr (Armee): 1) Erstes Training mit der Führungsunterstützungsbasis des Heeres 2) Start des gemeinsamen Masterstudiengangs EPFL ETHZ VBS 3) Erste EPFL-VBS-Schulungen 4) "Cyber Defense Curriculum" eingeführt	umgesetzt
M23	Nutzung der im Kontext vom NDG entwickelten Kapazitäten von FUB-ZEO: 1) Die geplanten Aktivitäten sind mit Fachämtern auf unerwünschte Kollateraleffekte abgesprochen 2) Die Kapazitäten sind vorhanden	umgesetzt
M24	Projektabschluss «Aufbau Cyber»	umgesetzt

4.9 Handlungsfeld 9 «Aktive Positionierung der Schweiz in der internationalen Cyber-Sicherheitspolitik»

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M25 Aktive Mitgestaltung und Teilnahme an Prozessen der Cyber-Aussensicherheitspolitik (EDA, SECO)
- M26 Internationale Kooperation zum Auf- und Ausbau von Kapazitäten im Bereich Cyber-Sicherheit (EDA)
- M27 Bilaterale politische Konsultationen und multilaterale Dialoge zu Cyber-Aussensicherheitspolitik (EDA)

Status der Umsetzung:



Meilensteine 2018 – Q2 2021

	Meilensteine	Status
M25	Teilnahme an UNO Prozessen: 1) Jährliche Berichterstattung 2019 und 2020	umgesetzt
	Interessenvertretung im Rahmen der OSZE (staatliche Vertrauensbildung): 1) Teilnahme an Verhandlungen sowie aktive Mitgestaltung des Prozesses und jährliche Berichterstattung 2019 und 2020	umgesetzt
	Aufbau und Etablierung des Geneva Dialogues on Responsible Behavior in Cyberspace: 1) Konzept für die Etablierung des Genfer Dialogs als Multistakeholder-Plattform 2) 2-3 Dialogrunden des Expert*innenprozesses zur Anwendung des Völkerrechts auf den Cyberraum haben stattgefunden 3) Erkenntnisse aus dem Expert*innenprozess werden in UNGGE und OEWG eingespeist 4) Schweizer Interessen im Bereich der Anwendung des Völkerrechts auf den Cyberraum sind in den Schlussberichten der UNGGE und der OEWG reflektiert	umgesetzt
	Verfolgung der Entwicklungen in der Europäischen Union (insbesondere im Europäischen Auswärtigen Dienst und ENISA): 1) Auslegeordnung der wichtigsten Akteure, Prozesse sowie Massnahmen der EU ist erstellt und das Engagement der Stellen der CH darin ist identifiziert 2) Mögliche Auswirkungen der verschiedenen EU-Massnahmen auf die Schweiz sind analysiert	umgesetzt
	Engagement zur Förderung eines offenen und freien Cyber-Raums: 1) Auslegeordnung der relevanten internationalen Menschenrechtsprozesse und Foren 2) Beurteilung zur Schweizer Teilnahme an ausgewählten Prozessen und Foren	umgesetzt

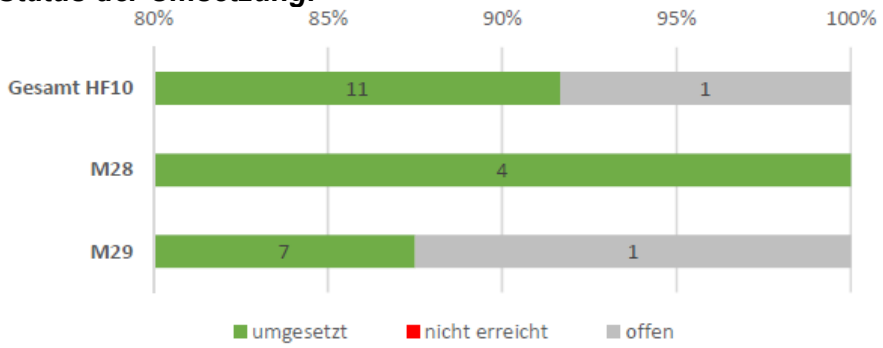
M26	Durchführung von Workshops mit regionalen Organisationen: 1) Konzepterstellung und Durchführung des ersten Workshops in Genf	umgesetzt
	Workshops zum Aufbau von Institutionen und Cyberaussensicherheits-strukturen: 1) Bedarfsanalyse, Training, Konzept, Durchführung 1. Workshop	umgesetzt
M27	Sino-European Cyber Dialogue (SECD): 1) Etablierung der Arbeitsgruppe International Law 2) Weiterführung des SECD	umgesetzt
	MENA Cybersecurity Forum: 1) Weiterführung des MENA Cybersecurity Forums	umgesetzt

4.10 Handlungsfeld 10 «Aussenwirkung und Sensibilisierung»

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M28 Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS (NCSC)
- M29 Sensibilisierung der Öffentlichkeit für Cyber-Risiken (NCSC)

Status der Umsetzung:



Meilensteine 2018 – Q2 2021

	Meilensteine	Status
M28	Erarbeitung eines Kommunikationskonzeptes zur NCS: 1) Situationsanalyse erstellt 2) Kommunikationskonzept NCS (Ziele, Zielgruppen, Botschaften, Zielumsetzung (Strategie), Instrumente/Massnahmen, Erfolgsmessung sowie Budget) erarbeitet 3) Kommunikations-Verantwortlichkeiten sowie –Termine (Plan) definiert, sowie Abstimmung hierzu mit weiteren NCS-Akteuren erfolgt 4) Start der Umsetzung des Kommunikationsplans	umgesetzt
M29	Entwicklung und Durchführung einer nationalen Awareness-Kampagne: 1) Abstimmung mit aktiven Akteuren zur konzeptionellen Erarbeitung einer nationalen Awareness-Kampagne durchgeführt 2) Konzept zur nat. Kampagne erstellt 3) Umsetzungsplan vorhanden 4) Start / Produktion der nationalen Kampagne	umgesetzt
	Informationsplattform zu Cyberrisiken: 1) Konzept für Plattform ist entwickelt (Inhalte) 2) Lancierung der Plattform über die Sensibilisierungskampagne 3) Auswertung der Nutzung der Plattform und Anpassung der Inhalte	umgesetzt