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

Stand erstes Quartal 2020

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Inhaltsverzeichnis

1 Vorwort ... 3
2 Übersicht Stand der Umsetzungsarbeiten ... 4
3 Stand Organisation zur Umsetzung ... 5
3.1 Übersicht zu den Beschlüssen des Bundesrats ... 5
3.2 Stand der Umsetzung der interdepartementalen Gremien und des NCSC ... 6
3.2.1 Cyberausschuss des Bundesrats ... 6
3.2.2 Der Delegierte des Bundes für Cybersicherheit ... 7
3.2.3 Kerngruppe Cyber ... 7
3.2.4 Steuerungsausschuss NCS ... 7
3.2.5 Nationales Zentrum für Cybersicherheit ... 7
4 Schwerpunkte der Umsetzung der NCS ... 9
4.1 Unterstützung der KMU beim Schutz vor Cyberrisiken ... 9
4.1.1 KMU-Schnelltest, Leitfaden und Cybersecurity Toolkit ... 9
4.1.2 Label Cyber Safe ... 10
4.2 Förderung von Forschung und Ausbildung ... 10
4.2.1 Berufsprüfung Cyber Security Specialist ... 10
4.2.2 CYD-Campus ... 11
4.2.3 «Swiss Support Centre for Cyber-Security» und Masterstudiengang der beiden ETH ... 11
4.3 Resilienz der kritischen Infrastrukturen ... 11
4.4 Standardisierung ... 12
4.4.1 Sicherheitsstandards für IoT-Geräte ... 12
4.4.2 IKT-Minimalstandards ... 12
4.5 Prüfung einer Meldepflicht ... 12
4.6 Verbesserte Koordination bei der Bekämpfung von Cybercrime ... 13
4.7 Ausbau der Zusammenarbeit mit Kantonen ... 13
4.8 Erneuerung der Public Private Partnership «Swiss Cyber Experts» ... 14
4.9 Geneva Dialogue on Responsible Behaviour in Cyberspace ... 14
5 Detaillierter Umsetzungsstand ... 15
5.1 Handlungsfeld 1 Kompetenzen- und Wissensaufbau ... 16
5.2 Handlungsfeld 2 Bedrohungslage ... 17
5.3 Handlungsfeld 3 Resilienz-Management ... 18
5.4 Handlungsfeld 4 Standardisierung / Regulierung ... 19
5.5 Vorfallbewältigung ... 20
5.6 Krisenmanagement ... 21
5.7 Strafverfolgung ... 22
5.8 Cyber-Defence ... 23
5.9 Aktive Positionierung der Schweiz in der internationalen Cyber-Sicherheitspolitik ... 24
5.10 Aussenwirkung und Sensibilisierung ... 25

1 Vorwort

Vor einem Jahr durfte ich meine Funktion als Delegierter des Bundes für Cybersicherheit aufnehmen. Ich habe wertvolle Einblicke in bestehende Prozesse und Zuständigkeiten erhalten und bin auf motivierte Frauen und Männer getroffen, die konstruktiv über Organisationsstrukturen hinweg zusammenarbeiten. Die Zusammenarbeit und der Austausch inner- und ausserhalb der Bundesverwaltung sind für mich denn auch zentral. Dies gilt explizit in Bezug auf die koordinierte Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) 2018-2022. Sie gibt die Ziele zum Schutz vor Cyberrisiken über alle Massnahmenbereiche vor. Die Umsetzung wird dabei wesentlich durch Akteure aus den Kantonen, der Wirtschaft, der Hochschulen und der Gesellschaft mitgetragen. Der Blick auf den Umsetzungsstand der NCS sowie die Massnahmen zur Verbesserung der Koordination zeigen, dass diese Zusammenarbeit gut funktioniert.

Seit der Verabschiedung der NCS 2018-2022 wurde die neue Organisation des Bundes im Bereich Cyberrisiken vom Bundesrat beschlossen und umgesetzt. Die Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung, die seit dem 1. Juli 2020 in Kraft ist, bildet die rechtliche Grundlage und regelt die Zusammenarbeit innerhalb der Bundesverwaltung sowie mit den Kantonen, der Wirtschaft und der Wissenschaft. Das Nationale Zentrum für Cybersicherheit NCSC ist operativ. Mit der Kerngruppe Cyber und dem Steuerungsausschuss NCS wurden die interdepartementalen Gremien geschaffen, um eine enge Koordination aller Akteure sicherzustellen.

In den verschiedenen Handlungsfeldern der NCS wurden wichtige Fortschritte erzielt. Bei der Förderung von Forschung und Ausbildung wurden etwa mit der Lancierung der neuen Berufsprüfung zum Cyber Security Specialist oder mit der Eröffnung des Cyber Defence Campus (CYD Campus) an den beiden ETH und in Thun wichtige Meilensteine erreicht. Die Unterstützung von kleinen und mittleren Unternehmen (KMU) im Bereich Cyberrisiken wird stetig ausgebaut. Das neu lancierte Label Cyber-safe.ch ermöglicht es KMU transparent und einheitlich ihren Stand in Sachen Cybersicherheit auszuweisen. Die Koordination bei der Bekämpfung von Cyberkriminalität konnte durch die Etablierung des Cyberboards, welches die wichtigsten Partner in der Strafverfolgung von Cyberkriminalität vereint, verbessert werden. In der Digitalaussenpolitik der Schweiz gewinnt die Cyberdiplomatie immer mehr an Bedeutung. Mit den USA konnte kürzlich ein erster Cyber-Dialog geführt werden. Auch der "Geneva Dialogue on Responsible Behavior in Cyberspace" wird weitergeführt.

Wir sind auf Kurs. Der Blick auf die NCS zeigt aber auch, es gibt noch viel zu tun. Ich sehe unter anderem innerhalb der Bundesverwaltung Aufholbedarf im Bereich des Grundschutzes und bei der Sensibilisierung und Weiterbildung von Mitarbeiterinnen und Mitarbeitern. Entscheidend scheint mir überdies zu sein, dass die Leistungen im Cyberbereich objektiv beurteilbar sind. Wir wollen Erfolge messbar machen und differenzierte Kritik ermöglichen. Dazu müssen wir klare Messkriterien definieren und einheitlich anwenden. Und, es steht ein richtungsweisender Entscheid an: Der Bundesrat will bis Ende 2020 einen Grundsatzentscheid betreffend die Einführung einer Meldepflicht fällen.
Cybersicherheit ist und bleibt ein Prozess und wir sind mittendrin. Für mich steht fest: Je besser und effizienter dabei die Zusammenarbeit aller Akteure ist, desto sicherer ist und wird die Schweiz in Bezug auf Cyberrisiken.

Florian Schütz

2 Übersicht Stand der Umsetzungsarbeiten

Im Umsetzungsplan der NCS werden in den 29 Massnahmen 247 Meilensteine definiert. Bis im ersten Quartal 2020 wurden 72 davon umgesetzt, 23 sind verzögert und 3 konnten nicht erreicht werden. Der Umsetzungsstand wird in Kapitel 5 detailliert beschrieben. Die untenstehende Übersicht gibt einen Eindruck über den Stand der Umsetzung und die weitere Meilensteinplanung.

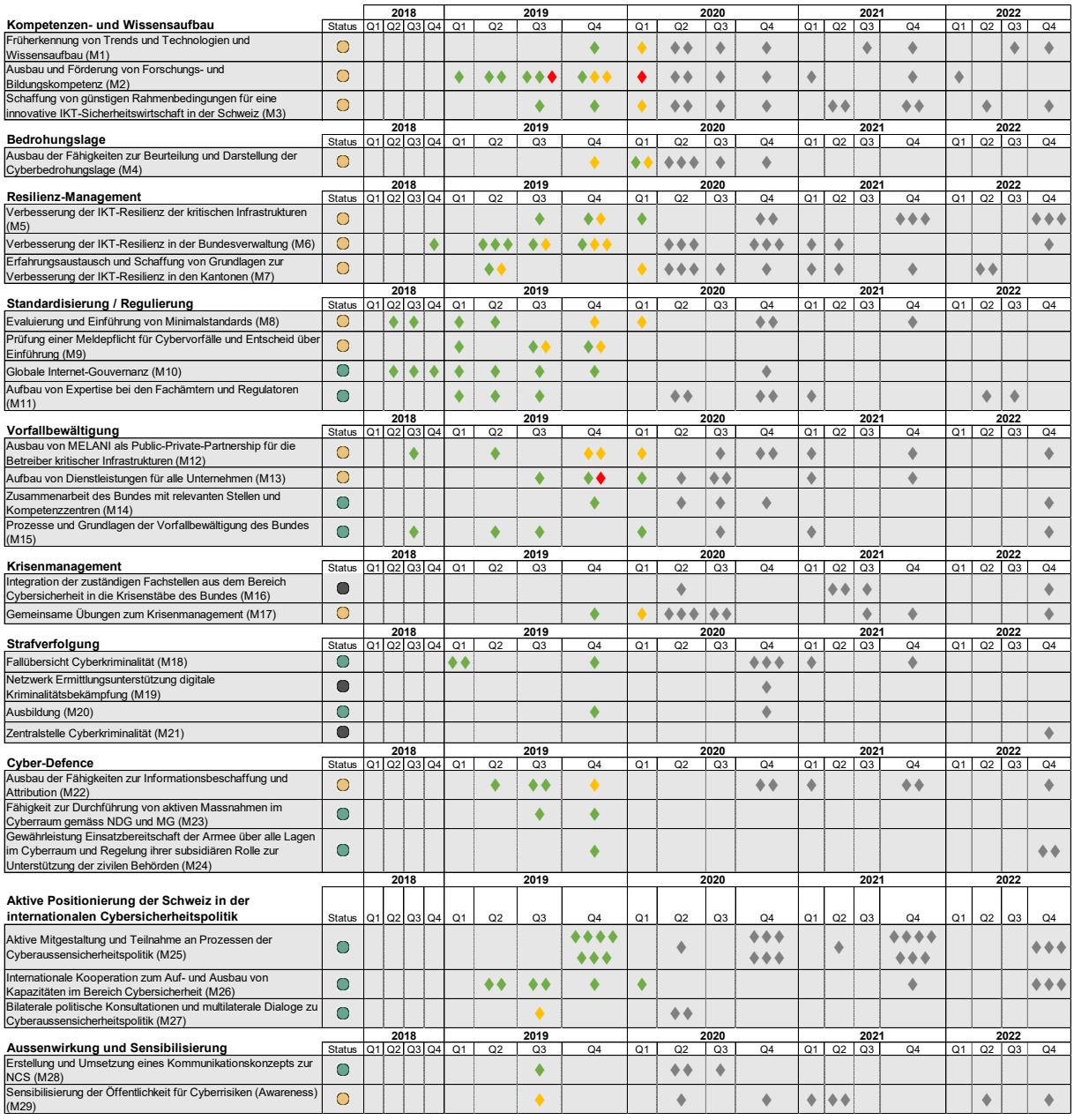


Abbildung 1 Übersicht Stand der Umsetzungsarbeiten

3 Stand Organisation zur Umsetzung

In mehreren Schritten wurde die Organisation des Bundes im Bereich Cyberrisiken über die letzten zwei Jahre neugestaltet. In diesem Kapitel werden die dazu nötigen Beschlüsse des Bundesrates aufgeführt und der Stand der Umsetzung der beschlossenen Organisation aufgezeigt.

3.1 Übersicht zu den Beschlüssen des Bundesrats

Nach der Verabschiedung der NCS 2018-2022 im April 2018 hat der Bundesrat verschiedene weitere Beschlüsse zur deren Umsetzung und zur Organisation des Bundes gefällt. Abbildung 2 fasst diese Beschlüsse zusammen.

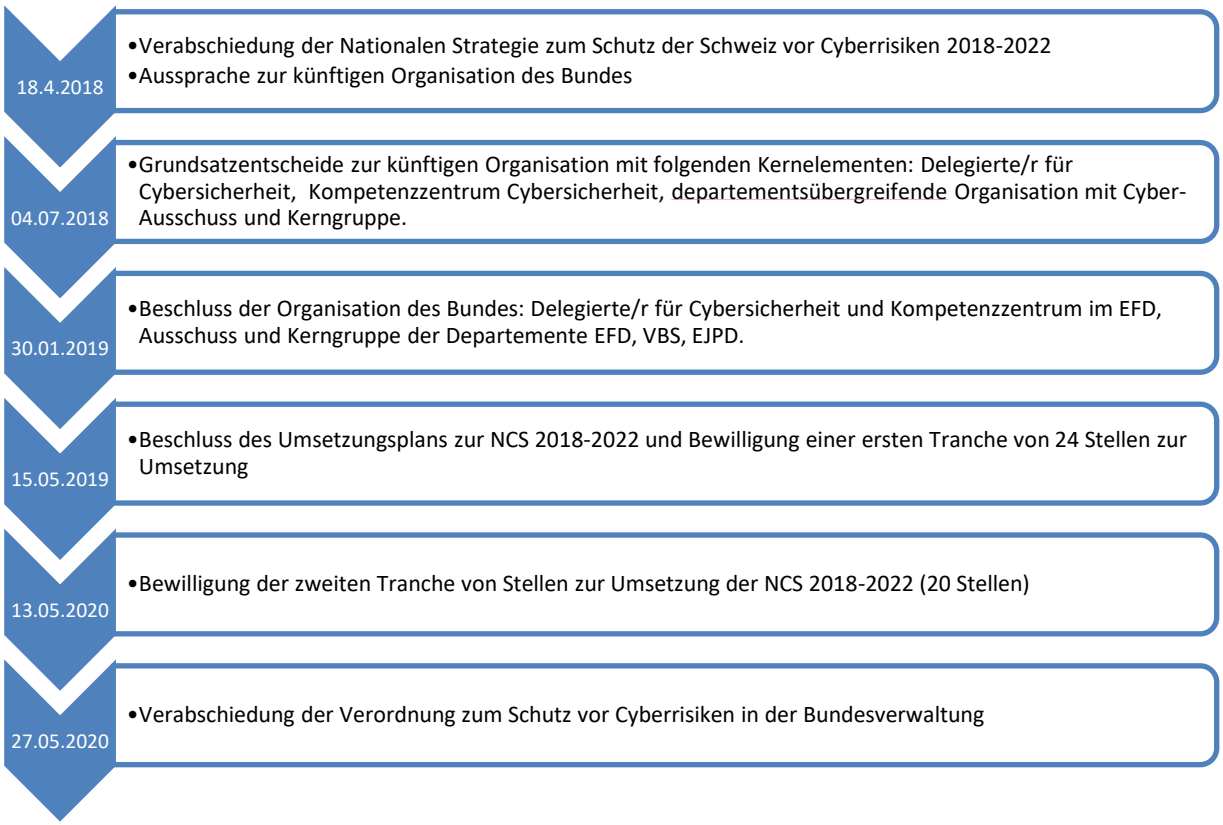


Abbildung 2 Übersicht Beschlüsse des Bundesrats

Zusätzlich zu diesen Beschlüssen hat der Bundesrat folgende Berichte als Antwort auf überwiesene Postulate zu Themen mit Bezug zur Cybersicherheit verabschiedet:

- 27.11.2019: Bericht über die Organisation des Bundes zur Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken; Bericht in Erfüllung der Postulate 16.4073 Golay vom 15.12.16 und 18.3003 SiK NR vom 22.01.18 und der Motion 17.3508 Eder vom 15.06.2017;
- 13.12.2019: Varianten für Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen. Bericht des Bundesrates in Erfüllung des Postulates 17.3475 Graf-Litscher vom 15.06.17;
- 29.04.2020: Sicherheitsstandards für Internet-of-Things-Geräte (IoT). Bericht des Bundesrates in Erfüllung der Postulate 17.4295 Glättli vom 15.12.2017 und 19.3199 Reynard vom 21.03.2019.

3.2 Stand der Umsetzung der interdepartementalen Gremien und des NCSC

Die Organisation des Bundes zum Schutz vor Cyberrisiken umfasst als Kernelemente drei interdepartementale Gremien (Cyberausschuss des Bundesrats, Kerngruppe Cyber, Steuerungsausschuss NCS), den oder die Delegierte/n für Cybersicherheit als zentrale Ansprechperson des Bundes und das Nationale Zentrum für Cybersicherheit (NCSC), als Kompetenzzentrum des Bundes.
Dieses Kapitel zeigt die Tätigkeiten der interdepartementalen Gremien und des Delegierten auf und beschreibt den Stand der Arbeiten beim Aufbau des Nationalen Zentrums für Cybersicherheit.

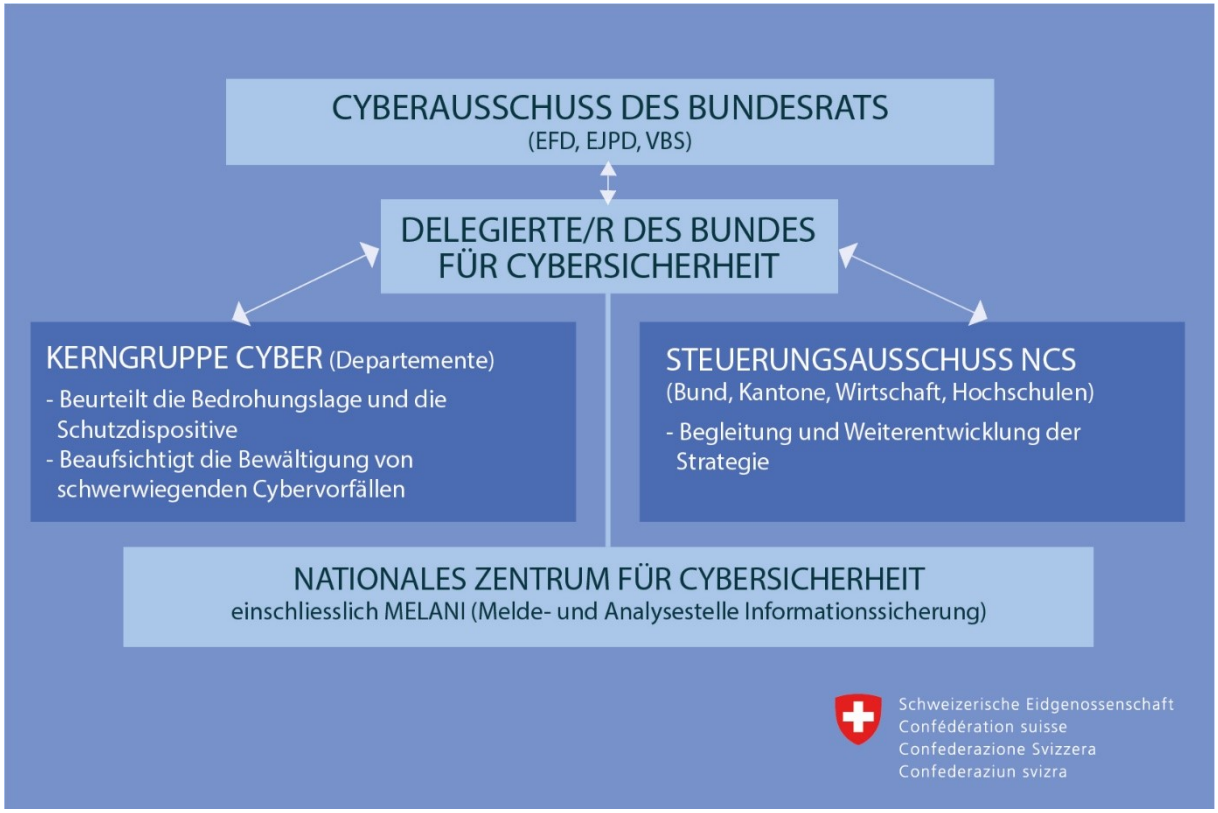


Abbildung 3 Organisation des Bundes im Bereich Cyberrisiken

3.2.1 Cyberausschuss des Bundesrats

Der Cyberausschuss des Bundesrats hat bis im Juni 2020 dreimal unter dem Vorsitz des Vorstehers des Eidgenössischen Finanzdepartements (EFD) getagt. Neben den Departementsvorstehenden des EFD, des Eidgenössischen Justiz- und Polizeidepartements (EJPD) und des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) nehmen jeweils auch der Präsident der Konferenz der Kantonalen Justiz und Polizeidirektorinnen und -direktoren (KKJPD) und der Delegierte des Bundes für Cybersicherheit an den Sitzungen teil. Der Ausschuss lässt sich über die aktuelle Bedrohungslage informieren, bespricht Geschäfte des Bundesrats mit Relevanz für die Cybersicherheit und erörtert strategisch-politische Fragestellungen.

3.2.2 Der Delegierte des Bundes für Cybersicherheit

Im August 2019 hat Florian Schütz[1] die Funktion des Delegierten des Bundes für Cybersicherheit übernommen. Er ist direkt dem Departementsvorsteher des EFD unterstellt und leitet die interdepartementalen Gremien zur Verbesserung der Koordination der Arbeiten im Bereich Cyberrisiken. Zudem steht er dem neu geschaffenen Nationalen Zentrum für Cybersicherheit (NCSC) vor, das als Kompetenzzentrum des Bundes für Cybersicherheit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen ist.

3.2.3 Kerngruppe Cyber

Die Kerngruppe Cyber setzt sich analog zum Cyberausschuss des Bundesrats aus den Departementen EFD (GS), EJPD (fedpol) und VBS (GS) und dem Präsidenten der Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS) zusammen. Den Vorsitz hat der Delegierte des Bundes für Cybersicherheit. Die Kerngruppe hat 2019 neunmal getagt. Sie bereitet die Sitzungen des Cyberausschusses vor und sorgt darüber hinaus für eine möglichst gute Koordination im Bereich Cyberrisiken. Um der Koordinationsaufgabe nachzukommen und um die Kerngruppe weiteren wichtigen Akteuren im Bereich verschiedener Cyberthemen zu öffnen, wurde beschlossen, ein erweitertes Format (KGCy+) einzuführen, in welchen es nicht um die direkte Vorbereitung von Sitzungen des Cyberausschusses geht,. In der erweiterten Kerngruppe ständig vertreten ist das Eidgenössische Departement für auswärtige Angelegenheiten EDA (Büro des Sondergesandten für Cyber-Aussen- und Sicherheitspolitik), weitere Akteure werden bei Bedarf durch den Delegierten eingeladen.

3.2.4 Steuerungsausschuss NCS

Der Steuerungsausschuss NCS sorgt für die strategische Kohärenz bei der Umsetzung der NCS-Massnahmen, koordiniert die beteiligten Akteure und prüft den Umsetzungsfortschritt laufend mittels strategischem Controlling. Erhat im November 2019 zum ersten Mal getagt. Vertreten sind jene Organisationen, welche direkt für die Umsetzung von Massnahmen der NCS zuständig sind. Es sind dies folgende Organisationen:

- Verwaltungseinheiten des Bundes: Nationales Zentrum für Cybersicherheit (NCSC), armasuisse W+T, Bundesamt für Bevölkerungsschutz (BABS), Bundesamt für Kommunikation (BAKOM), Bundeskanzlei (BK), Bundesamt für wirtschaftliche Landesversorgung (BWL), Büro Sondergesandter für Cyber-Aussen- und Sicherheitspolitik des EDA, Bundesamt für Polizei (fedpol), Generalsekretariat des Eidgenössischen Departement des Innern (EDI), Generalsekretariat des VBS, Nachrichtendienst des Bundes (NDB) und Führungsunterstützungsbasis der Armee (FUB);
- Kantone: Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD), Sicherheitsverbund Schweiz (SVS), Cyberboard;
- Wirtschaft: ICTswitzerland, Switch, Swiss Cyber Experts, Cyber-Safe;
- Hochschulen: ETH Zürich, ETH Lausanne.

3.2.5 Nationales Zentrum für Cybersicherheit

Das Nationale Zentrum für Cybersicherheit wird seit August 2019 im Generalsekretariat EFD als eigenständige Einheit aufgebaut. Kern des Zentrums bildet die Melde- und Analysestelle Informationssicherung MELANI, welche in das NCSC übergeht. 2019 wurden folgende Teile

[1] Florian Schütz verfügt über einen Master in Computerwissenschaft sowie einen Master of Advanced Studies in Sicherheitspolitik und Krisenmanagement der ETH Zürich und hat mehr als 10 Jahre Führungserfahrung im Bereich der IT-Sicherheit in der Privatwirtschaft.

des Zentrums auf- und ausgebaut:

- Nationale Anlaufstelle für Meldungen zu Vorfällen und Fragen zu Cyberrisiken: Die Anlaufstelle ist seit 1. Januar 2020 operativ in Betrieb. Die Meldestelle nimmt seither durchschnittlich 200 Meldungen pro Woche entgegen, führt eine erste Analyse dieser Meldungen durch und leitet sie wenn nötig an die zuständigen Stellen weiter.
- Das GovCERT als nationales Computer Emergency Response Team wurde personell gestärkt.
- Die Geschäftsstelle des NCSC wurde ausgebaut.

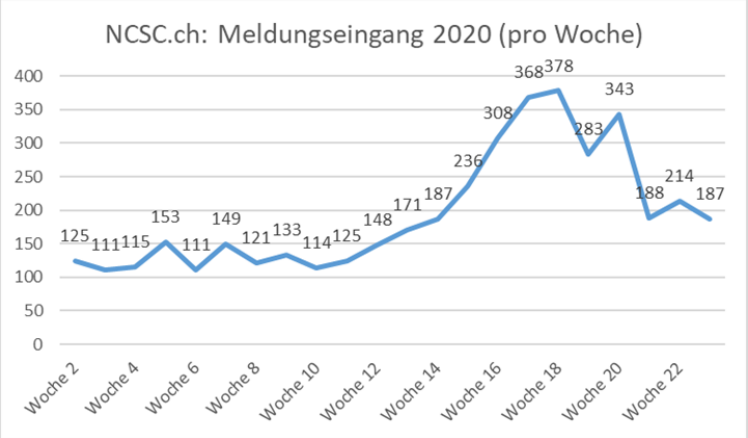


Abbildung 4 Anzahl Meldungen pro Woche (Stand Mai 2020)

Ab 2020 wird im NCSC ein Expertenpool aufgebaut, welcher die Fachämter bei cyberspezifischen Projekten unterstützt sowie den Bereich «Sensibilisierung der Öffentlichkeit» stärkt.

4 Schwerpunkte der Umsetzung der NCS

Parallel zur Neugestaltung der Organisation 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 Gesellschaft mitgetragen. Während in Kapitel 5 die erreichten Meilensteine in allen Handlungsfeldern kurz beschreiben werden, soll im vorliegenden Kapitel auf Schlüsselprojekte der aktuell laufenden Arbeiten eingegangen werden.

4.1 Unterstützung der KMU beim Schutz vor Cyberrisiken

Kleine und mittlere Unternehmen (KMU) waren nicht unter der Zielgruppe der ersten NCS 2012-2017. Entsprechend existieren bislang nur wenige national koordinierte Massnahmen zur Unterstützung von KMU in diesem Bereich. Mit der Umsetzung der NCS 2018-2022 werden in verschiedenen Handlungsfeldern Projekte angegangen, um diese Situation zu verbessern.

4.1.1 KMU-Schnelltest, Leitfaden und Cybersecurity Toolkit

In einer breit abgestützten Initiative[2] wurde 2018 ein Schnelltest für KMU zum Thema Cybersicherheit erarbeitet. Ziel der Initiative ist es, ein Instrument zur Selbstbeurteilung insbesondere auch für kleinere Unternehmen zur Verfügung zu stellen. Mit dem Schnelltest[3] kann auch ein Unternehmen mit weniger ausgeprägten Kenntnissen bezüglich Informatik und IT-Sicherheit unkompliziert und schnell feststellen, ob die technischen, organisatorischen und mitarbeiterbezogenen Massnahmen zum Schutz vor Cyberrisiken ausreichend sind.

Mit der Veröffentlichung des Tests haben KMU den Bedarf nach konkreten Anleitungen zur Verbesserung ihrer Cybersicherheit angemeldet. Als Reaktion darauf wurde unter der Leitung von ICTswitzerland und der Schweizerischen Akademie der Technischen Wissenschaften (SATW) – wiederum unter Beteiligung von Experten des Bundes und der Wirtschaft – ein Leitfaden[4] für die Umsetzung eines minimalen Grundschutzes erstellt. Zudem wurde mit der Global Cyber Alliance (GCA) eine Vereinbarung getroffen, damit deren Inhalte (konkrete und kostenlose Werkzeuge inklusive Anleitung)[5] übersetzt und Schweizer KMU zur Verfügung gestellt werden können.

Abbildung 5 Global Cyber Security Alliance

[2] Die Initiative wird getragen von ICTSwitzerland, der Information Security Society Switzerland (ISS), der Schweizerischen Akademie der Technischen Wissenschaften (SATW), dem Schweizerischen Normenverband (SNV), der Schweizerischen Vereinigung für Qualitäts- und Managementsysteme, dem Schweizerischen Versicherungsverband und Vertretungen des Bundes.

[3] abrufbar unter www.cybersecurity-check.ch

[4] abrufbar unter: https://ictswitzerland.ch/content/uploads/2020/03/Leitfaden_Cybersecurity_Schnelltest_D.pdf

[5] abrufbar unter: https://gcatoolkit.org/de/kmu/

4.1.2 Label Cyber Safe

Fehlende oder zu komplexe Standards verhindern, dass KMU transparent ihren Stand im Bereich Cybersicherheit beurteilen und diesen auch gegenüber Dritten ausweisen können. Das durch den Schweizer Verband für das Cybersecurity-Gütesiegel (Association suisse pour le Label de Cybersécurité, ASLaC) entwickelte Cyber Safe-Gütesiegel soll dem entgegenwirken. Das Label ist eine private Initiative und wurde in enger Zusammenarbeit mit Vertretern von KMU entwickelt[6]. Es wurde am 18. Dezember 2019. lanciert und leistet einen wichtigen Beitrag zur Umsetzung der NCS. Alle Informationen zum Label sind auf www.cyber-safe.ch verfügbar.

Abbildung 7 Cyber-Safe.ch

4.2 Förderung von Forschung und Ausbildung

Im Handlungsfeld 1 «Kompetenzen und Wissensaufbau» konnten wichtige Fortschritte erzielt werden. Mit der neuen Berufsprüfung «Cyber Security Specialist» wurde ein neuer Abschluss geschaffen, welcher den Fachkräftemangel zu entschärfen hilft. Das Projekt wurde von der Armee als Bestandteil der Arbeiten zur Schaffung eines Cyber-Lehrgangs Armee vorangetrieben und ist ein gutes Beispiel der konstruktiven Zusammenarbeit zwischen zivilen und militärischen Stellen.
Wichtig ist auch die Eröffnung des Cyber Defence Campus (CYD Campus) an den beiden ETH und in Thun, als wissenschaftlich-technisches Kompetenzzentrum. Der Campus wird den Wissenstransfer zwischen Behörden und Akademie verbessern und dazu beitragen, dass in der Schweiz ein wirtschaftliches Ökosystem für Cybersicherheit entsteht. Hierzu trägt ebenfalls das sich im Aufbau befindende «Swiss Support Centre for Cyber-Security» (SSCC) der beiden ETH bei, welches eine koordinative Rolle im Sinne einer Anlaufstelle für Bund und Kantone einnimmt. .

4.2.1 Berufsprüfung Cyber Security Specialist

Am 11.11.2019 lancierte die nationale Organisation der Arbeitswelt ICT-Berufsbildung Schweiz die Berufsprüfung zum «Cyber Security Specialist (CSS)»[7]. Berufsprüfungen mit Eidgenössischem Fachausweis stellen den ersten Abschluss der tertiären Stufe in der Berufsbildung dar. Zur Berufsprüfung zugelassen werden KandidatInnen, die eine Berufsausbildung mit Eidgenössischem Fähigkeitszeugnis abgeschlossen haben und mindestens 2 Jahre Berufspraxis im Bereich der Informationssicherheit oder Cyber-Sicherheit verfügen.
Die Entwicklung der Berufsprüfung wurde von der Armee mitfinanziert und soll einen zusätzlichen Anreiz für SoldatInnen bilden, sich für den Cyber-Lehrgang der Armee zu bewerben. Erfolgreiche AbsolventInnen dieses Lehrgangs werden nämlich für die Berufsprüfung zugelassen, wenn sie mindestens ein Jahr Berufspraxis im Bereich der Informationssicherheit oder Cybersicherheit verfügen.

[6] Vertretung der KMU durch Fédération des Entreprises Ro-mandes Neuchâtel (FER Neuchâtel), Chambre de commerce, d'industrie et des services de Genève (CCIG), Fédération Patronale et Economique Fribourg (FPE-CIGA), Chambre vaudoise du commerce et de l'industrie (CVCI), Chambre valaisanne de commerce et d'industrie, Association Suisse des Cadres (ASC/SKO), Association Femmes PME Suisse romande, Groupement Suisse de l'Industrie Mécanique (GIM-CH);
Zudem waren auch die Zivilgesellschaft (iCON NGO), Hochschulen und ETH (HEIG-VD, HES-SO Wallis, EPFL C4DT) sowie Gemeinden (Waadtländer Gemeinden) vertreten.

[7] Weiter Infos: https://www.ict-berufsbildung.ch/berufsbildung/ict-weiterbildung/cyber-security-specialist-efa/

4.2.2 CYD-Campus

Der Cyber-Defence Campus (CYD-Campus) wurde im Januar 2019 bei armasuisse W+T mit dem Zweck gegründet, Cyberentwicklungen möglichst frühzeitig zu antizipieren, Cybertechnologien zu entwickeln und zu prüfen sowie Cyberfachkräfte aus- und weiterzubilden. Er übernimmt die Funktion eines Bindeglieds zwischen den Behörden, der Industrie und der Wissenschaft in Forschung, Entwicklung und Ausbildung für die Cyberabwehr. Neben dem Standort in Thun konnten im September 2019 und im November 2019 die Standorte an der EPFL und an der ETH Zürich eröffnet werden.
Der CYD Campus veranstaltet regelmässig Konferenzen zu Themen im Bereich der Cyberabwehr und vergibt in Zusammenarbeit mit der EPFL Fellowships zur Forschung im Bereich Cyberverteidigung.

4.2.3 «Swiss Support Centre for Cyber-Security» und Masterstudiengang der beiden ETH

Die beiden ETH haben sich gemeinsam verpflichtet ein «Swiss Support Centre for Cyber-Security» (SSCC) zu schaffen. Das Zentrum soll den Austausch zwischen der Forschung an den ETH und den Behörden fördern und dazu beitragen, dass die Spitzenforschung der beiden Hochschulen möglichst direkt die Cybersicherheit in der Schweiz verbessert. Die Finanzierung des Zentrums ist geregelt und die ersten beiden Mitarbeiter haben ihre Arbeit aufgenommen. Das Zentrum wird weiter ausgebaut und wird seine verschiedenen im Umsetzungsplan beschriebenen Beiträge zur NCS leisten.
Seit dem Studienjahr 2019/2020 bieten die beiden ETH zudem einen gemeinsamen Masterstudiengang in Cybersicherheit an. Die Studieninhalte umfassen Kryptografie, Hardware-, Software- und Netzwerksicherheit sowie Methoden zur Gewährleistung von Systemsicherheit und Nutzervertrauen. Der Studiengang beinhaltet auch Praxiselemente und beschränkt sich nicht nur auf technischen Aspekten der Cybersicherheit, sondern deckt auch die ethischen, rechtlichen und betrieblichen Fragen in diesem Fachgebiet ab.

4.3 Resilienz der kritischen Infrastrukturen

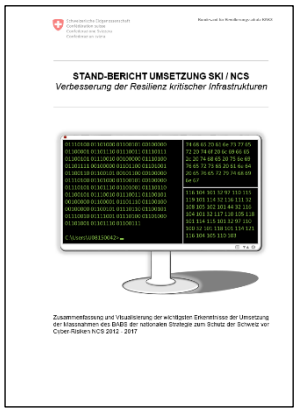


Abbildung 8 Bericht Umsetzung Resilienz der KI

Das Bundesamt für Bevölkerungsschutz (BABS) hat auf der Basis der von 2012 - 2017 erstellten Risiko- und Verwundbarkeitsanalysen einen Statusbericht zur Resilienz der kritischen Infrastrukturen der Schweiz verfasst. Der Bericht stellt eine Momentaufnahme der geschätzten Risiken und laufenden Massnahmen zur Verbesserung der Resilienz dar. Die gewonnenen Erkenntnisse helfen, Cyberrisiken im Kontext der gesamten Gefährdungslage der kritischen Infrastrukturen besser einzuordnen. Der Zusammenzug der Informationen ermöglicht es zudem, übergreifende Probleme zu erkennen und damit Synergien in der Bearbeitung besser nutzbar zu machen.
Die gewonnenen Erkenntnisse bieten Entscheidungsträgern eine Grundlage für die Priorisierung der verschiedenen möglichen Resilienz-Massnahmen in den kritischen Teilsektoren.

Koordiniert durch das Bundesamt für Bevölkerungsschutz BABS werden im Rahmen der Umsetzung der zweiten NCS von 2018-2022 alle bestehenden Risiko- und Verwundbarkeitsanalysen aktualisiert und bei Bedarf neue Resilienz-Massnahmen abgeleitet. Die im Rahmen der ersten NCS-Periode bereits beschlossenen und laufenden Resilienz-Massnahmen werden gemäss den vereinbarten Verantwortlichkeiten weitergeführt.

4.4 Standardisierung

Im Handlungsfeld Standardisierung und Regulierung sind ein Bericht zu Sicherheitsstandards bei IoT-Geräten verfasst und weitere Minimalstandards für kritische Sektoren erarbeitet worden.

4.4.1 Sicherheitsstandards für IoT-Geräte

Der Bericht «Sicherheitsstandards für IoT-Geräte» beschreibt, welche Herausforderungen in Bezug auf die Sicherheit von Systemen mit IoT-Komponenten bestehen, welche internationalen Standards bei der Sicherung solcher Systeme angewendet werden können und welche rechtlichen Grundlagen heute in der Schweiz gelten. Der Bericht wurde als Antwort auf die beiden Postulate 17.4295 Glättli und 19.3199 Reynard verfasst.[8] Er soll als Grundlage für die weiteren Arbeiten in diesem Bereich dienen.

4.4.2 IKT-Minimalstandards

Der IKT-Minimalstandard dient als Empfehlung und mögliche Orientierungshilfe zur Verbesserung der IKT-Resilienz von Unternehmen. Er richtet sich insbesondere an die Betreiber von kritischen Infrastrukturen, ist aber grundsätzlich für jedes Unternehmen oder jede Organisation anwendbar und frei verfügbar[9].

Um die Anwendung dem Minimalstandard in kritischen Sektoren zu erleichtern, werden durch die Branchenverbände in Zusammenarbeit mit dem Bundesamt für wirtschaftliche Landesversorgung branchenspezifische Standards ausgearbeitet. Für die Sektoren Strom, Lebensmittel, Wasserversorgung und Abwasser sind solche Branchenstandards bereits entwickelt worden.

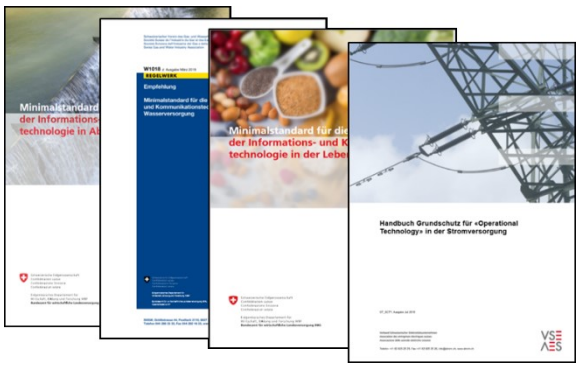


Abbildung 9 IKT-Minimalstandards

4.5 Prüfung einer Meldepflicht

Der Bundesrat hat im Dezember 2019 den Bericht «Varianten für Meldepflichten für kritische Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen» verabschiedet.[10] Der Bericht, mit welchem der Bundesrat das Postulat 17.3475 Graf-Litscher beantwortet, zeigt Varianten der Einführung von Meldepflichten auf. Diese wurden auf Basis der heute bereits bestehenden Meldepflichten für Sicherheitsvorfälle, den Erkenntnissen aus Interviews mit Expertinnen und Experten und den Analysen von Meldepflichten in anderen Ländern entwickelt. Wesentlich für die möglichen Varianten ist die Frage, ob Cybervorfälle einer separaten Stelle gemeldet werden müssen oder ob die in den Sektoren teilweise schon bestehenden Meldestellen für Sicherheitsvorfälle ergänzt werden sollen. Abhängig von dieser Organisationsstruktur ist zu

[8] https://www.ncsc.admin.ch/melani/de/home/dokumentation/berichte.html

[9] https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

[10] https://www.ncsc.admin.ch/melani/de/home/dokumentation/berichte.html

beurteilen, ab welchem Ausmass und unter welchen Voraussetzungen Vorfälle meldepflichtig sind, welche Fristen für die Meldungen gelten, ob Meldungen anonym abgegeben werden können und ob Sanktionen für den Unterlassungsfall definiert werden. Der Bundesrat hat das NCSC zusammen mit dem Bundesamt für Bevölkerungsschutz (BABS) beauftragt, diese Fragen unter Einbezug der zuständigen Behörden, der Kantone und des Bundes sowie der Wirtschaft abzuklären. Dabei ist auch zu prüfen, ob eine Ausweitung der generellen Meldepflichten für Funktionsausfälle bei kritischen Infrastrukturen vorgenommen werden soll. Bis Ende 2020 will der Bundesrat Grundsatzentscheide über die Einführung von Meldepflichten fällen.

4.6 Verbesserte Koordination bei der Bekämpfung von Cybercrime

Mit dem Cyberboard etablierte die Strafverfolgung gemeinsam mit den Partnerbehörden eine nationale Arbeitsmethode für den Wissenstransfer und die strategische sowie operative Koordination bei der Bekämpfung von Cybercrime. Das Cyberboard besteht aus dem strategischen Steuerungsorgan Cyber-STRAT und einem operativen Bereich, welcher aus Cyber-CORE (Kernelement; koordinative Aufgaben) sowie Cyber-CASE (Fallübersicht) und Cyber-STATE (Lagebild) besteht. Das Cyberboard vereinte 2019 regelmässig die wichtigsten Akteure der Strafverfolgung von Cybercrime, insbesondere auch das Spezialistennetzwerk NEDIK (Netzwerk Ermittlungsunterstützung Digitale Kriminalitätsbekämpfung). Dadurch konnte die Zusammenarbeit im vergangenen Jahr intensiviert werden. Insbesondere bei umstrittenen Zuständigkeitsfragen konnten Gerichtsstandskonflikte vermieden und schnelle sowie einvernehmliche Lösungen gefunden werden, was der Bekämpfung von Cybercrime zu Gute kommt.
Des Weiteren hat, als Grundlage für die operative Zusammenarbeit, jede Staatsanwaltschaft einen Cyber-SPoC (Single Point of Contact) nominiert. Im Rahmen dieser operativen Koordination konnte die Strafverfolgung die nationale Koordination bei Cyber-Phänomenen, wie z.B. falschen Immobilienanzeigen oder Ransomware-Angriffen gegen Unternehmen, verbessern. Die polizeiliche Zusammenarbeit wird durch NEDIK gefördert. Dieses Netzwerk hat sich gut etabliert und wird weiter ausgebaut. Zur systematischen und strukturierten Erfassung von Fällen digitaler Kriminalität hat eine Gruppe von westschweizer Kantonen die Plattform PICSEL (Plateforme d'Information de la Criminalité Sérielle en Ligne) entwickelt. Aktuell läuft die Testphase für diese Plattform. Damit verfügt die Strafverfolgung über wichtige Voraussetzungen, um im Sinne der Verbundsaufgabe die Fähigkeiten zur Cybercrime-Bekämpfung laufend weiterzuentwickeln und die NCS-Massnahmen umzusetzen.

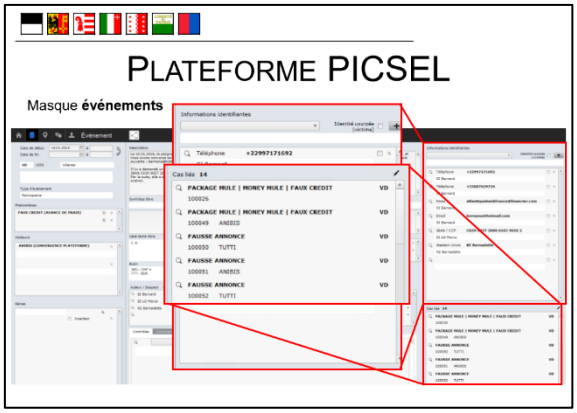


Abbildung 10 Plattform PICSEL

4.7 Ausbau der Zusammenarbeit mit Kantonen

Als Reaktion auf den Entscheid des Bundesrats, ein nationales Zentrum für Cybersicherheit aufzubauen, haben mehrere Kantone ihr Interesse daran bekundet und ihre Unterstützung angeboten. 2019 fanden erste Gespräche mit interessierten Kantonen statt, in welchen erörtert wurde, wie die in den Kantonen vorhandenen Kompetenzen im Bereich Cybersicherheit besser mit den Arbeiten des Bundes vernetzt werden können.

Die Politische Plattform des Sicherheitsverbund Schweiz (SVS) hat in der Folge ihren Delegierten im März 2020 beauftragt, eine Bestandsaufnahme kantonaler Kompetenzen und Projekte zu erstellen, um einen Überblick zu erhalten und die Grundlagen für eine strukturierte Zusammenarbeit zwischen dem NCSC und den Kantonen zu entwickeln.

4.8 Erneuerung der Public Private Partnership «Swiss Cyber Experts»

Im ersten Quartal 2020 wurde der neue Kooperationsvertrag zwischen der Eidgenossenschaft und dem Verein Swiss Cyber Experts (SCE) unterzeichnet, mit der Option um Verlängerung um weitere fünf Jahre. Der Verein wird das NCSC bei der Analyse von Vorfällen unterstützen, zum Lagebild des Bundes beitragen und bei Bedarf weitere Unterstützungsarbeiten zu Gunsten der Cybersicherheit der Schweiz übernehmen.

Abbildung 11 Logo Swiss Cyber Experts

4.9 Geneva Dialogue on Responsible Behaviour in Cyberspace

In der Aussenpolitischen Strategie 2020-23[11] identifiziert der Bundesrat die Digitalisierung als einen neuen Schwerpunkt der Schweizer Aussenpolitik. Die Cyberdiplomatie wird hierbei als ein zentrales Element der Digitalaussenpolitik definiert. Ziel der Cyberdiplomatie ist die Interessenwahrung im Cyberraum (bzw. im digitalen Raum). Dafür will die Schweiz ihr internationales Engagement intensivieren und ihr Profil im Bereich der Cyberdiplomatie weiter ausbauen.
Bestandteil dieser Aktivitäten ist der «Geneva Dialogue on Responsible Behaviour in Cyberspace». Der Dialog wurde Ende 2018 gemeinsam mit DiploFoundation, United Nations Institute for Disarmament Research (UNIDIR), der ETH Zürich und der Universität Lausanne lanciert. Im Mai 2020 wurde die zweite Phase des Dialogs eingeläutet. Hierbei steht der Dialog zwischen globalen Unternehmen über gute Praktiken (Best Practices) für mehr Produktsicherheit im Cyberraum im Zentrum. Neben Schweizer Unternehmen wie etwa UBS und SwissRe nehmen u.a. auch Microsoft (USA), Cisco (USA), Kaspersky (RUS), Sberbank (RUS), Huawei (China), Siemens (DE), FireEye (USA) und VU Security (ARG) teil. Das Projekt wird vom EDA in Zusammenarbeit mit dem WEF, der ETH Zürich sowie der Swiss Digital Initiative durchgeführt.

[11] https://www.eda.admin.ch/eda/de/home/das-eda/umsetzung-aussenpolitik/aussenpolitischestrategie.html

5 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 ersten Quartal 2020 erreicht oder nicht erreicht wurden. Zudem werden die Meilensteine kurz beschrieben, damit klar ist, um welchen Beitrag es sich dabei handelt.
Insgesamt wurden von den 247 im Umsetzungsplan der NCS definierten Meilensteine 72 umgesetzt, 23 sind verzögert und 3 wurden bislang nicht erreicht.[12] Mit einem Umsetzungsstand von nicht ganz einem Drittel nach 9 von total 20 Quartalen Laufzeit der NCS lässt sich feststellen, dass die Umsetzung der NCS generell auf Kurs ist, wenn auch in den meisten Massnahmen ein Grossteil der Arbeiten noch ansteht. Abbildung 11 verdeutlicht den Umsetzungsstand über alle Meilensteine hinweg.

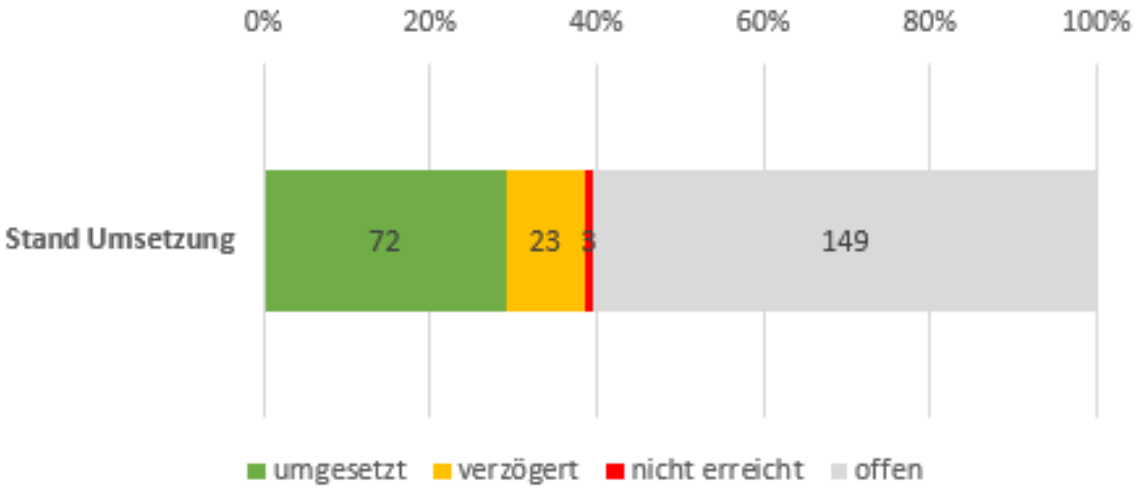


Abbildung 12 Umsetzungsstand der NCS-Meilensteine

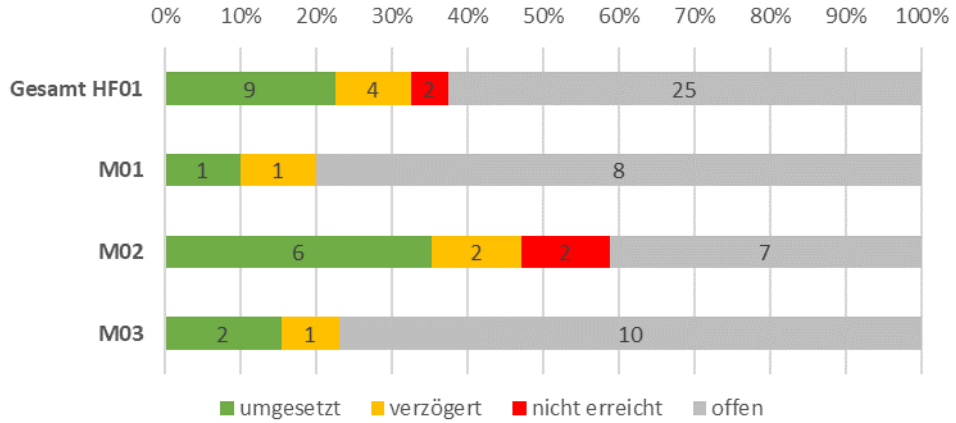
[12] Eine Verzögerung wird dann ausgewiesen, wenn der Meilenstein nicht rechtzeitig erfüllt werden konnte, die Umsetzungsverantwortlichen aber plausibel darlegen können, dass die Umsetzung nicht gefährdet ist.

5.1 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 – Q1 2020

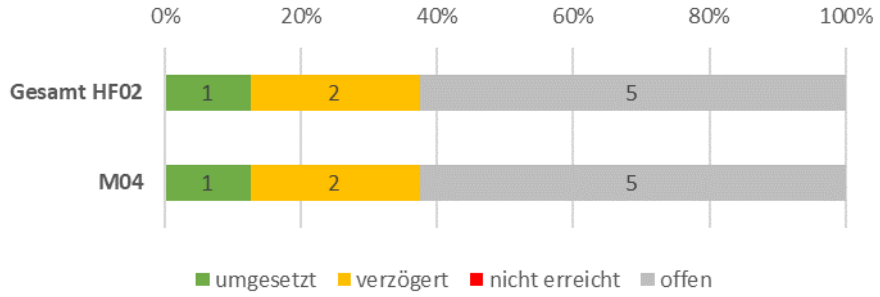
	Meilenstein	Status
M1	Technologiemonitoring: Leistungen des CYD Campus für das Monitoring zuhanden des NCSC sind festgelegt	Umgesetzt
	Trendanalyse: Konzept für Zielpublikum, Inhalte, Verbreitung der Berichte ist erstellt	verzögert
M2	Bedarfsanalyse zu Bildungsangebote: Analyse erstellt und Zielgruppen sind definiert	verzögert
	Forschungs- und Supportzentrum der beiden ETH: Konzept für das Forschungs- und Supportzentrum ist erstellt	umgesetzt
	Forschungs- und Supportzentrum der beiden ETH: Fragen der Finanzierung und Lokalität sind geklärt	umgesetzt
	CYD Campus Standort Thun nimmt Betrieb auf	umgesetzt
	CYD Campus Standort EPFL nimmt Betrieb auf	umgesetzt
	CYD Campus Standort ETHZ nimmt Betrieb auf	umgesetzt
	Wichtigste Forschungsinstitute im Bereich Cyberrisiken sind identifiziert	verzögert
	Etablierte Anlässe im Bereich «Ethical Hacking» sind identifiziert	umgesetzt
	Förderinstrumente sind ausgestaltet; Finanzmittel, wenn nötig beantragt und Fördermittel stehen zur Verfügung	Nicht erreicht. Massnahme: Projektänderung. Finanzierung durch Bund ist nicht das geeignete Mittel, Anlässe im Bereich Ethical Hacking zu fördern
M3	Ökosystem Cybersicherheit: Wichtigste Forschungsinstitute der Schweizer Hochschulen im Bereich Cyberrisiken sind identifiziert	verzögert
	Think Tank: Konzept für das Forschungs- und Supportzentrum der beiden ETH ist erstellt	umgesetzt
	Think Tank: Fragen der Finanzierung und Lokalität für das Forschungs- und Supportzentrum der beiden ETH sind geklärt	umgesetzt

5.2 Handlungsfeld 2 Bedrohungslage

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

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

Status der Umsetzung:



Meilensteine 2018 – Q1 2020

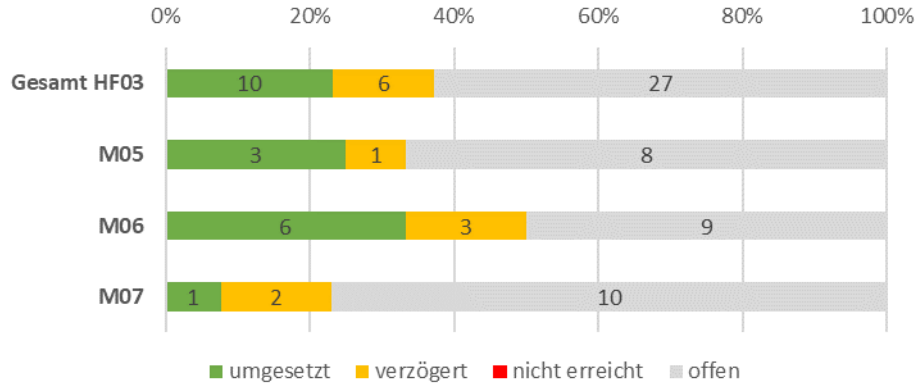
	Meilenstein	Status
M4	Bedarfsanalyse erstellt und Zielgruppen sind definiert	umgesetzt
	Leistungskatalog: Aufgabenbereich zw. Bund und Wirtschaft geklärt	verzögert
	Quellen: Liste zusätzlich benötigter Quellen erstellt	umgesetzt

5.3 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[13])

Status der Umsetzung:



Meilensteine 2018 – Q1 2020

	Meilenstein	Status
M5	Bestandsaufnahme der umgesetzten und noch nicht umgesetzten Vorhaben aus den Massnahmenberichten erstellt	umgesetzt
	Verantwortlichkeiten für die Umsetzung sind geklärt	umgesetzt
	Roadmap/Planung der laufenden und anstehenden Massnahmen erarbeitet	umgesetzt
	Etablierung einer akademischen Arbeitsgruppe für Cybersicherheit	verzögert
M6	Sicherheitsvorgaben: Bestehenden sicherheitsrelevanten Aufgaben und Ergebnisse in Projektmethoden analysiert	verzögert
	Grobkonzept Sensibilisierungskampagne IKT-Sicherheit in der Bundesverwaltung «SIB 19» erstellt (Q4/2018)	umgesetzt
	Start der Sensibilisierungskampagne IKT-Sicherheit in der Bundesverwaltung «SIB»	umgesetzt
	Abstimmung mit aktiven Akteuren zur konzeptionellen Ausdehnung zu einer nationalen Kampagne durchgeführt (siehe M29 «Sensibilisierung der Öffentlichkeit für Cyber-Risiken»)	verzögert
	Erstellung eines weiteren Massnahmenplans Sensibilisierung für die Jahre 2021/2022	verzögert
	SCION: Absichtserklärung interessierter Bedarfsträger und Pilotanwendern	umgesetzt
	SOC: Konzept und Umsetzungsplan	umgesetzt
	SOC: Umsetzung abgeschlossen	verzögert

[13] Informationen zu weiteren Projekten des Umsetzungsplans der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022 vom SVS und deren Umsetzungsstand finden Sie hier: https://www.svs.admin.ch/content/svs-internet/de/themen-/cybersicherheit/cybersicherheit-kantone/_jcr_content/contentPar/downloadlist_1137108093/downloadItems/145_1588841512416.download/Jahresbericht%20zum%20Stand%20der%20Projekte%20im%20Umsetzungsplan%20der%20Kantone.pdf

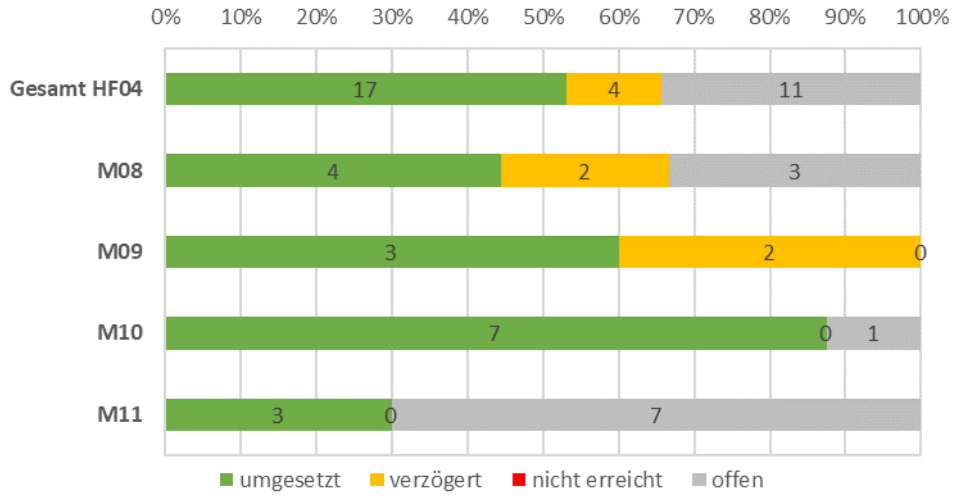
	Schnittstelle zu ETH: Koordination mit dem Delegierten für Cybersicherheit	umgesetzt
M7	Austausch Kantone: Anforderungsklärung der Arbeitsplatzausstattung bei NCSC	verzögert
	Durchführung der Cyber-Landsgemeinde	umgesetzt
	Schnittstelle ETH zu Kantonen: Koordination mit dem SVS	verzögert

5.4 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 – Q1 2020

	Meilenstein	Status
M8	Publikation des IKT-Minimalstandards und Hilfsmittel für das Assessment	umgesetzt
	Minimalstandard «Handbuch Grundschutz» des Verbands Schweiz. Elektrizitätsunternehmen (VSE)	umgesetzt
	Branchenstandard Trinkwasser und Lebensmittel	umgesetzt
	Branchenstandard Erdgas	verzögert
	Branchenstandard Öffentlicher Verkehr	verzögert
	Publikation Cybersecurity-Schnelltest für KMU (SATW) [Q3/2018]	umgesetzt
	Bedarfsanalyse zu weiteren Hilfsmittel (technische Hilfsmittel, Labels, Leitfäden, Anleitungen) für KMU	umgesetzt
M9	Ausschreibung und verfassen Grundstudie	umgesetzt
	Berichterstattung (Postulatbericht)	umgesetzt
	Weiterführende Diskussion mit Wirtschaft und Politik	verzögert
	Grundlage für Entscheid zur Meldepflicht	verzögert
M10	Treffen des hochrangigen Panels des UN-Generalsekretärs (New York, Genf, Helsinki)	umgesetzt

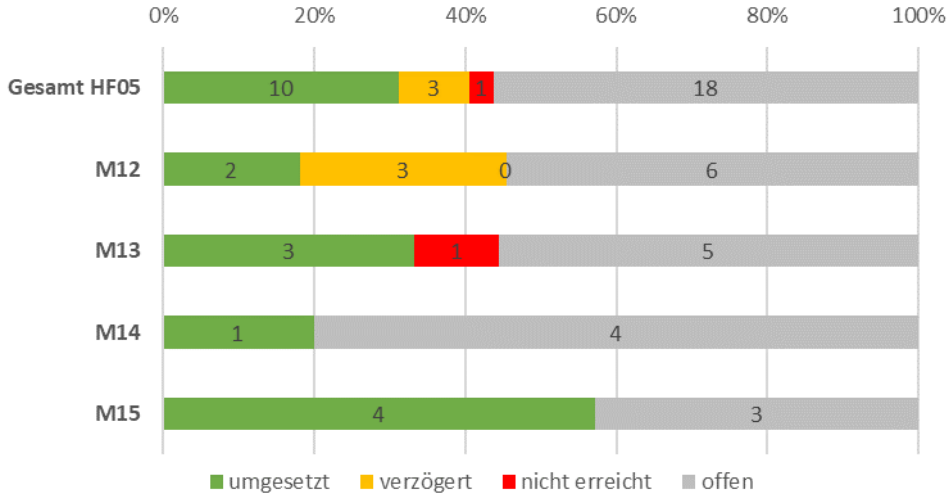
	Bericht des Panels	umgesetzt
	Evaluation Umsetzungsmöglichkeiten des Berichts	umgesetzt
M11	Expertenpool: Bedarfsabklärung	umgesetzt
	Expertenpool: Schaffung von Stellen für den Pool	umgesetzt
	Konzept der Gemeinsamen Forschungs- und Unterstützungsstelle EPFL-ETHZ erstellt	umgesetzt

5.5 Vorfallbewältigung

Übersicht Handlungsfeld: Massnahmen und Umsetzungsverantwortung

- M12 Ausbau von MELANI als Public-Private-Partnership für die Betreiber 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 – Q1 2020

	Meilenstein	Status
M12	GK MELANI: Situationsanalyse über Nutzung von MELANI durch die verschiedenen kritischen Sektoren ist erstellt	verzögert
	Studie mit Variantenempfehlung zu MELANI-NET 2.0 erstellt (Q3/2018)	umgesetzt
	PoC (Proof of Concept) zur empfohlenen Variante durchgeführt	umgesetzt
	Konzept MELANI-NET 2.0	verzögert
	MELANI-NET 2.0 ist produktiv	verzögert
M13	Nationale Anlaufstelle Cyber: Grobkonzept für das Online-Portal für die Meldung von Cybervorfällen erstellt	umgesetzt
	Situations- und Bedarfsanalyse zu möglichen «Best Practices» zur Cybervorfallbewältigung erstellt	nicht erreicht. Massnahme: Änderung der Projektplanung. Integration weiterer Partner.
	Anforderungsklärung bezüglich Alarmierung, Warnung und Information der Öffentlichkeit im Cybervorfall erfolgt -> Alertswiss-App	umgesetzt

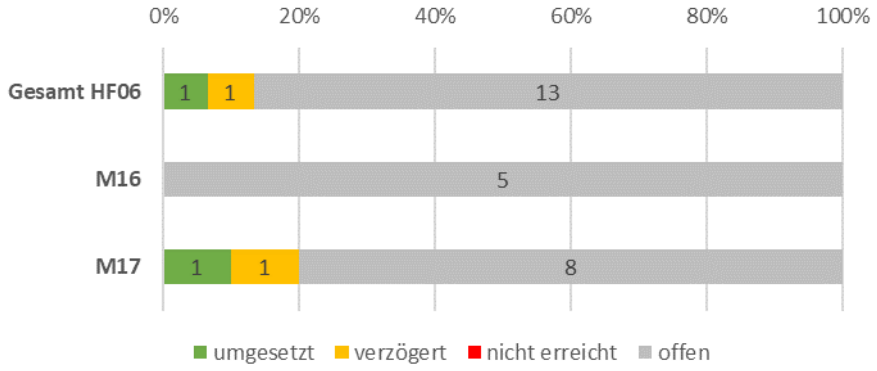
	Konzept zur Integration der Cyber-Informationen im Alert-swiss-App ist erstellt	umgesetzt
M14	Erhebung der bestehenden operativen SOCs und CERTs inklusive Ansprechpartner durchgeführt und dokumentiert	umgesetzt
M15	Erarbeitung Cyberverordnung	umgesetzt
	Beschluss der Verordnung durch Bundesrat	umgesetzt
	Inkrafttreten der Verordnung festgelegt	umgesetzt
	Erster Entwurf für einen Vorfallbewältigungsprozess im Bund, Diskussion mit Leistungserbringern und betroffenen Stellen	umgesetzt

5.6 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 – Q1 2020

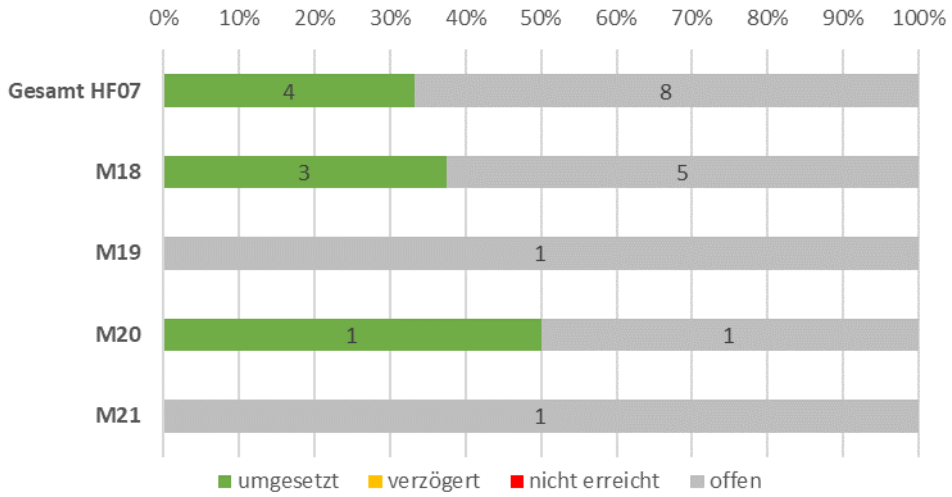
	Meilenstein	Status
M16	Keine Meilensteine bis Q1 2020	
M17	Bestandaufnahme bestehender und geplanten nationalen und internationalen Krisenübungen mit Cyberaspekten	verzögert
	Bedarfsanalyse zu sektorspezifischen Krisenübungen ist erfolgt	umgesetzt

5.7 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 – Q1 2020

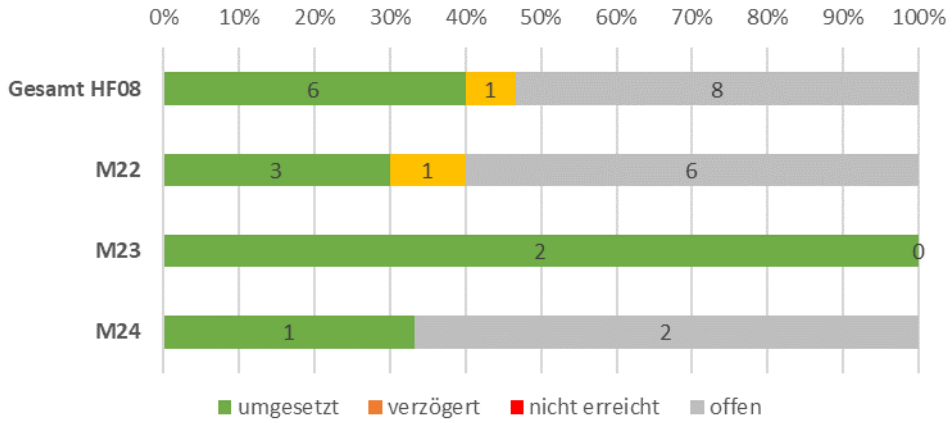
	Meilenstein	Status
M18	Fallübersicht Cyberkriminalität: Testphase PICSEL gestartet	umgesetzt
	Tool Cyber-CASE; Fallkomplex-Liste sämtlicher Cyber-SPoC-StA (bereits operativ)	umgesetzt
	Monatliches Bulletin (polizeilich) NEDIK	umgesetzt
M19	Keine Meilensteine bis Q1 2020	
M20	Übersicht der Akad. Ausbildungsmöglichkeiten (polizeilich)	umgesetzt
M21	Keine Meilensteine bis Q1 2020	

5.8 Cyber-Defence

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 – Q1 2020

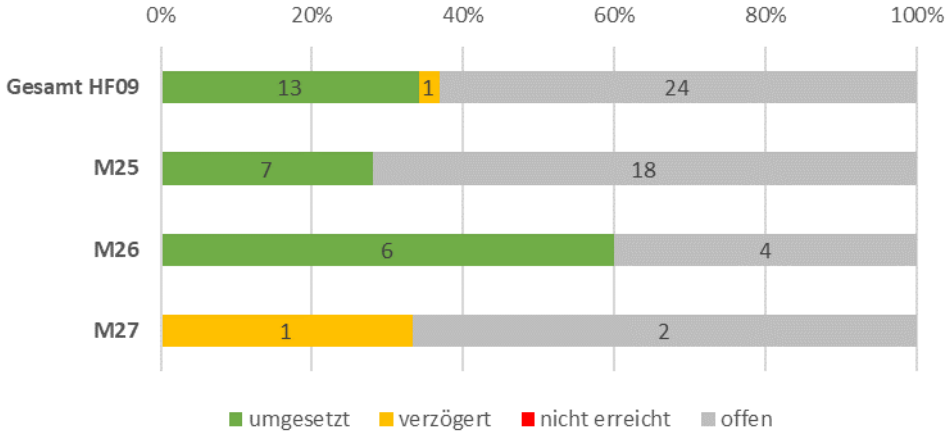
	Meilenstein	Status
M22	Fähigkeiten zur Informationsbeschaffung und Attribution: Ausbau erste Etappe ist erfolgt	verzögert
	Ausbildung: Erstes Training mit der Führungsunterstützungsbasis des Heeres	umgesetzt
	Start des gemeinsamen Masterstudiengangs EPFL ETHZ VBS	umgesetzt
	Erste EPFL-VBS-Schulungen	umgesetzt
M23	FUB-ZEO Kapazitäten: Die geplanten Aktivitäten sind mit Fachämtern auf unerwünschte Kollateraleffekte abgesprochen	umgesetzt
	Die Kapazitäten sind vorhanden	umgesetzt
M24	Projektabschluss «Aufbau Cyber»	umgesetzt

5.9 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 – Q1 2020

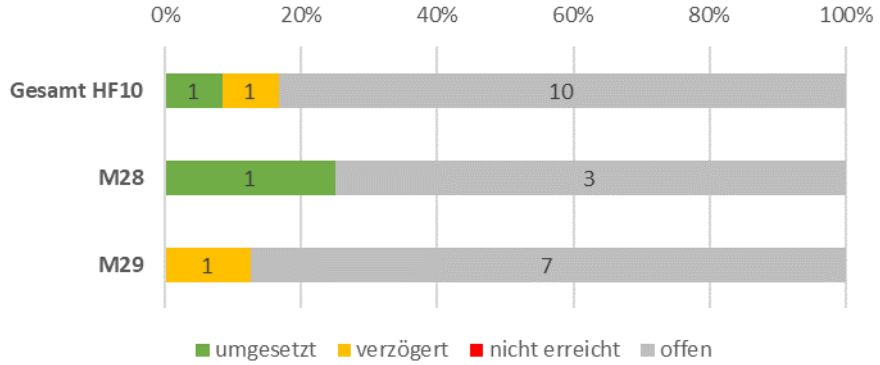
	Meilenstein	Status
M25	Teilnahme an UNO Prozessen: Jährliche Berichterstattung	umgesetzt
	OSZE: Teilnahme an Verhandlungen sowie aktive Mitgestaltung des Prozesses und jährliche Berichterstattung	umgesetzt
	Konzept für die Etablierung des Genfer Dialogs als Multistakeholder-Plattform	umgesetzt
	2-3 Dialogrunden des Expertenprozesses zur Anwendung des Völkerrechts auf den Cyberraum haben stattgefunden	umgesetzt
	Auslegeordnung der wichtigsten Akteure, Prozesse sowie Massnahmen der EU ist erstellt und das Engagement der Stellen der CH darin ist identifiziert	umgesetzt
	Auslegeordnung der relevanten internationalen Menschenrechtsprozesse und Foren	umgesetzt
M26	Internationale Kooperation: Konzepterstellung und Durchführung des ersten Workshops in Genf	umgesetzt
	Workshops zum Aufbau von Institutionen und Cyberaussensicherheitsstrukturen: Bedarfsanalyse, Training, Konzept, Durchführung 1. Workshop	umgesetzt
M27	Sino-European Cyber Dialogue (SECD): Weiterführung des SECD	verzögert

5.10 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 – Q1 2020

	Meilenstein	Status
M28	NCSC Kommunikationskonzept: Situationsanalyse erstellt	umgesetzt
M29	Abstimmung mit aktiven Akteuren zur konzeptionellen Erarbeitung einer nationalen Awareness-Kampagne durchgeführt	verzögert