Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation

12. Januar 2021

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

Informationen zum Inhalt

In diesem Dokument werden folgende Themen behandelt:
- Anforderungen an eine Cyber-Organisation im Kanton und deren Aufgaben, Kompetenzen, Verantwortlichkeiten und Prozesse
- Schnittstellen mit den Cyber-Strukturen des Bundes.

Das Konzept wurde von der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) am 12. November 2020 verabschiedet.

1. Zusammenfassung

Cyber ist ein Querschnittsthema, das sowohl Behörden (Verwaltung, Gerichte etc.), Kritische Infrastrukturen als auch weitere Institutionen sowie die Bevölkerung betrifft. Prävention und Sensibilisierung sowie die Vorbereitung auf einen Cyber-Vorfall sind deshalb zentral. Denn ein solcher Vorfall kann nicht mehr nur durch eine Organisation bewältigt werden. Cybereignisse sind kantons- und länderübergreifend. Es wird ein vernetztes und im Ereignisfall ein schnelles Denken und Handeln gefordert. Die Sofortmassnahmen nach einem Angriff müssen rasch und wirkungsvoll umgesetzt werden. Das vorliegende Konzept mit empfehlendem Charakter legt dar, welche Strukturen und Aufgaben für die Prävention und die Erhöhung der Cyber-Sicherheit im Verbund mit weiteren Akteuren im Kanton empfohlen werden.

Folgende Vorteile resultieren aus der Umsetzung dieses Konzepts:

- Eine Ansprechstelle für alle Cyber-Belange des Kantons, die zugleich auch den Bundesbehörden als *Single Point of Contact (SPoC)* zur Verfügung steht.
- Der Datendiebstahl- und/oder -abfluss kann verhindert oder gemindert werden.
- Die Informations- und Kommunikationstechnik-Mittel funktionieren weiterhin oder fallen nur teilweise aus.
- Die Geschäftsprozesse funktionieren weiterhin oder fallen nur teilweise aus.
- Die Kosten für eine Vorfallbewältigung sind tief, ein grosser Finanz- oder Imageverlust für die Verwaltung kann verhindert werden.
- Die Vernetzung zu anderen involvierten Stellen, insbesondere Kantone und dem Bund, ist sichergestellt.
- MELANI kann die kantonale Verwaltung bei einem Vorfall unterstützen.
- Die kritischen Infrastrukturen (KIs) sind geschützt.
- Die Wiederherstellung von Daten und Informationen ist in Kürze möglich.
- Die Wiederherstellung der IKT-Infrastruktur (Hardware- und Software inkl. Netzwerk) ist möglich.

2. Einleitung

Das vorliegende Konzept ist Teil der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022 und des dazugehörenden Umsetzungsplans der Kantone. Bei der Erarbeitung dieses Umsetzungsplans sprachen sich die Kantonsvertretenden ausdrücklich für die Massnahme zur Schaffung der kantonalen Organisationen für Cyber-Sicherheit aus: «Analog zur neu geschaffenen Organisationsstruktur im Cyber-Bereich auf Stufe Bund beabsichtigt diese Massnahme die Schaffung kantonaler Organisationen für Cyber-Sicherheit.»[1] Diese kantonale Stelle sollte mit Budgethoheit und Weisungsbefugnis ausgestattet sein und sie «(...) behält zu jeder Zeit den Überblick, repräsentiert den Kanton in Cyber-Belangen, vertritt ihn im Kantonalen Führungsstab und gewährleistet die Schnittstellen innerhalb des Kantons, zwischen den Kantonen und zum Bund.»[2] Der Bundesratsbeschluss zur Organisation des Bundes im Bereich Cyber-Risiken vom 30. Januar 2019 hält zudem nochmals explizit den Ausbau und die Vertiefung der Zusammenarbeit mit den Kantonen, der Wirtschaft und den Hochschulen zum Schutz vor Cyber-Risiken fest. Der Bundesrat hat auch die Schaffung eines Nationalen Kompetenzzentrums für Cyber-Sicherheit (NCSC) beschlossen. Die dafür vorgesehenen Strukturen dienen dem kantonalen Modell als Grundlage. Komplementär zur NCS hat der Bundesrat die Strategie zum Schutz kritischer Infrastrukturen (SKI)[3] für den Zeitraum 2018–2022 verabschiedet, auf welche das vorhandene Cyber-Konzept ebenfalls Bezug nimmt.

Die Konzeption zur Schaffung von kantonalen Organisationsstrukturen für Cyber-Sicherheit wurde von einer Arbeitsgruppe des Sicherheitsverbunds Schweiz mit Spezialisten aus verschiedenen Bereichen wie Informationstechnologie, Polizei, Bevölkerungsschutz aus der gesamten Schweiz zur Implementation des vorhergehenden erwähnten kantonalen Umsetzungsplans für den Zeitraum bis 2022 erarbeitet. Die folgenden Kapitel sind als Hilfestellung für die Einführung einer kantonalen Cyber-Organisation zu verstehen und erheben nicht den Anspruch auf Vollständigkeit; entsprechend kann das Konzept den jeweiligen kantonalen Erfordernissen und Bedürfnissen angepasst werden.

1 Informatiksteuerungsorgans des Bundes (ISB). *Umsetzungsplan zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022*, S. 78.
2 Ebd., S. 78.
3 Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022 (BBl 2018 503).

3. Gegenstand und Geltungsbereich

Das vorliegende Konzept kann die Grundlage für einen entsprechenden Regierungsratsbeschluss / eine Regelung bilden, um die Cyber-Organisation in einem Kanton zu implementieren. Die Aufgaben, Kompetenzen und Verantwortung sind in diesem Dokument beschrieben.

Dieses Konzept dient als Empfehlung sowohl für die ganze kantonale Verwaltung als auch für andere Organisationen wie Spitäler, Universitäten etc. insbesondere, wenn sie am gleichen Netzwerk wie die Behörden angeschlossen sind.

4. Ziele

- Vermeidung eines Cyber-Angriffs durch geeignete Massnahmen, bspw. durch die Identifikation, den Schutz, die Detektion, die Reaktion und die Wiederherstellung.
- Minimierung des Schadens (finanziell und Image) nach einem Angriff und raschmöglichste Betriebsaufnahme der wichtigsten Geschäftsprozesse.
- Die adäquate Ablauf- und Aufbauorganisation sind genehmigt, eingeführt und geübt.
- Sicherstellung des Zugangs zu einer stufengerechten Sensibilisierung und Schulung für alle Mitarbeitenden der Verwaltung.

5. Cyber-Organisation

5.1 Cyber-Organisation des Bundes[4]

- **Cyberausschuss des Bundesrats:** Er setzt sich aus den Vorstehenden der Departemente Eidgenössisches Finanzdepartement (EFD), Eidgenössisches Justiz- und Polizeidepartement (EJPD) und Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) zusammen und hat die Aufgabe, die Umsetzung der NCS zu beaufsichtigen.
- **Delegierter des Bundes für Cybersicherheit:** Der Delegierte ist direkt dem Departementsvorsteher des EFD unterstellt und Ansprechperson für Politik, Medien und Bevölkerung für Fragen, welche Cyberrisiken betreffen. Er steht dem Nationalen Zentrum für Cybersicherheit (NCSC) vor, leitet die interdepartementalen Gremien zur Verbesserung der Koordination der Arbeiten im Bereich Cyberrisiken und vertritt den Bund in weiteren Gremien.
- **Kerngruppe Cyber:** Sie stärkt die Koordination zwischen den drei Bereichen Sicherheit, Defence und Strafverfolgung, sorgt für eine gemeinsame Beurteilung der Bedrohungslage und beaufsichtigt die Bewältigung von schwerwiegenden und departementsübergreifenden Vorfällen durch die Bundesstellen. Vertretende der Kantone können situativ eingeladen werden.
- **Steuerungsausschuss NCS (StA NCS):** Er stellt die koordinierte und zielgerichtete Umsetzung der NCS-Massnahmen sicher und erarbeitet Vorschläge zur Weiterentwicklung der NCS. In diesem Gremium nehmen sowohl Vertretende des Bundes als auch der Kantone (KKJPD und SVS) sowie der Wirtschaft und der Hochschulen Einsitz.

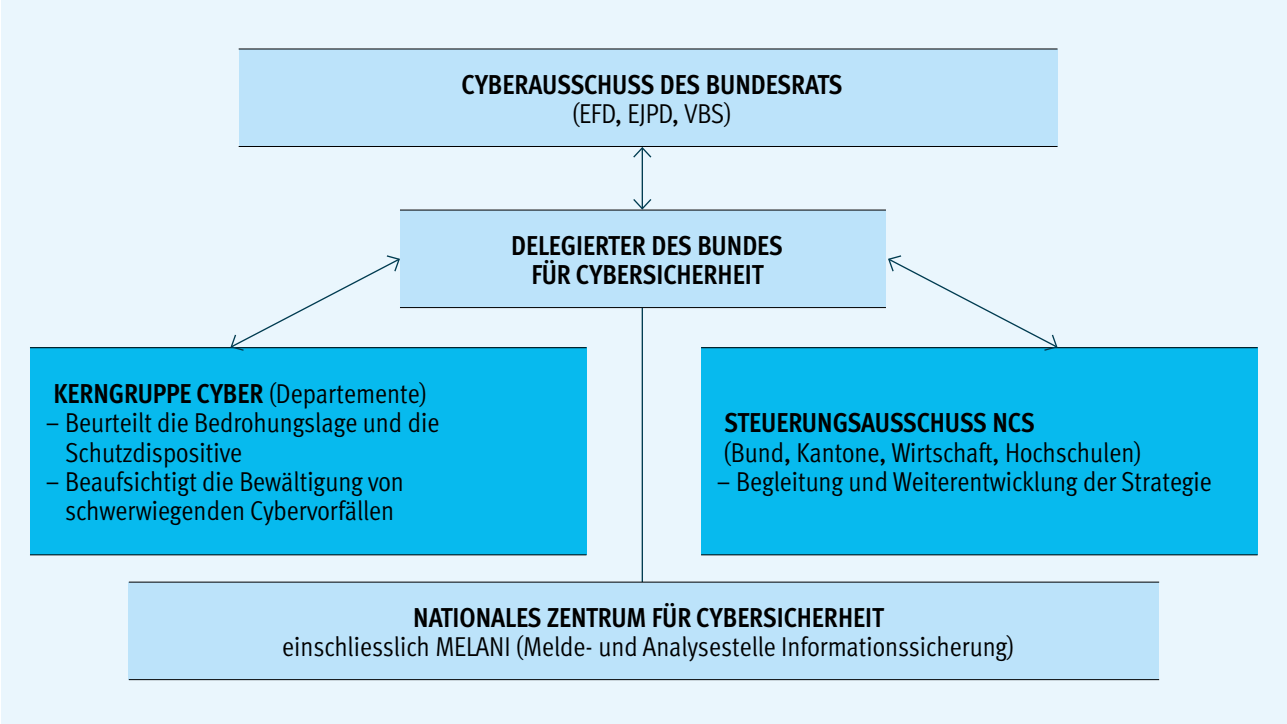

Abbildung 1: Cyber-Organisation Bund[1]

4 Nationales Zentrum für Cybersicherheit (NCSC): https://www.ncsc.admin.ch/ncsc/de/home/ueber-ncsc/das-ncsc.html (Stand: 07.01.2021).

– **Nationales Zentrum für Cybersicherheit:**
  Dieses Zentrum nimmt folgende Aufgaben wahr:
  - Nationale Anlaufstelle für Meldungen zu Vorfällen und Fragen zu Cyberrisiken für Behörden, private Unternehmen und die Bevölkerung.
  - Betrieb des nationalen Computer Emergency Response Team (GovCERT) als technische Fachstelle
  - Operative Führung der Vorfallbewältigung bei gravierenden Cybervorfällen
  - Geschäftsstelle des Delegierten für Cybersicherheit
  - Fachstelle für die IKT-Sicherheit des Bundes
  - Betrieb eines Expertenpools zur Unterstützung der Fachämter bei der Entwicklung und Umsetzung von Standards zur Cybersicherheit
  - Zusammenarbeit mit Wissenschaft und Forschung
  - Internationale Zusammenarbeit auf Fachebene

Das Nationale Zentrum für Cybersicherheit befindet sich derzeit im Aufbau. Allenfalls werden die Kantone Leistungen zugunsten dieses Zentrums erbringen können.[5]

5.2 Weitere zuständige Bundesorgane

Mit der Schaffung der Funktion des Cyber-Delegierten des Bundes wurde zugleich ein Single Point of Contact (SPoC) geschaffen, der u.a. als Ansprechstelle für die Bundesbehörden dient. Partner der nationalen Ebene sind namentlich die folgenden:

Bundesamt für Bevölkerungsschutz (BABS): Gemeinsam mit dem Bundesamt für wirtschaftliche Landesversorgung fördert das Bundesamt für Bevölkerungsschutz die Resilienz (Widerstands- und Regenerationsfähigkeit) von kritischen Infrastrukturen mit gezielten Massnahmen. Zentral ist insbesondere der Schutz von Informations- und Kommunikationsinfrastrukturen.[6]

Bundesamt für wirtschaftliche Landesversorgung (BWL): Als zuständige Organisation für die Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen in schweren Mangellagen, denen die Wirtschaft nicht selber zu begegnen vermag[7], hat das BWL den Minimalstandard zur Verbesserung der IKT-Resilienz[8] erlassen. Zwar sind die jeweiligen Unternehmen und Organisationen selbst für ihren Schutz verantwortlich, jedoch besteht eine gesetzliche Verantwortung, wenn der (Regel-)Betrieb von kritischen Infrastrukturen betroffen ist. Die Standards lassen sich auch für andere Bereiche und Unternehmen anwenden.

Melde- und Analysestelle Informationssicherung (MELANI): Die Aufgabe von MELANI ist die Früherkennung von Gefahren und deren Bewältigung sowie die Unterstützung der Betreiber von kritischen Infrastrukturen in der Krise. MELANI betreibt dafür das Computer Emergency Response Team (GovCERT), welches u.a. Dienstleistungen wie technische Analysen und Informationen über gezielte Attacken von KIs erbringt, und das Operation Information Center OIC, zuständig für die Analyse der Lage. Zudem fungiert MELANI als «Nationale Anlaufstelle» um Meldungen zu Cybervorfällen entgegen zu nehmen. Diese Anlaufstelle ist beim «Nationalen Zentrum für Cybersicherheit» an-

5 Im Rahmen eines Projekts unter der Leitung des Sicherheitsverbunds Schweiz wird im Jahr 2020 eine Bestandsaufnahme der kantonalen Leistungen durchgeführt und abgeklärt, wie ihre Kompetenzen anderen Dienstleistungsbezügern bereitgestellt werden können.
6 Bischof, Angelika P. «Betreiber kritischer Infrastrukturen sind gefordert», in: *Bevölkerungsschutz 27 (2017)*, S. 13–15.
7 Die rechtlichen Grundlagen der Wirtschaftlichen Landesversorgungen bilden der Art. 102 der Bundesverfassung und das Landesversorgungsgesetz.
8 Bundesamt für landwirtschaftliche Versorgung (2018). *Minimalstandard zur Verbesserung der IKT-Resilienz*, unter: https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html (Stand: 07.01.2021).

gesiedelt, die erste Anlaufstelle für Fragen im Bereich Cyberrisiken ist.[9]

Bundesanwaltschaft (BA): Die BA ist einerseits für klassische Staatsschutzdelikte, d.h. für Straftaten, die sich gegen den Bund richten oder dessen Interessen stark betreffen, zuständig. Anderseits obliegt der BA die Strafverfolgung von komplexen interkantonalen bzw. internationalen Fällen von organisierter Kriminalität (einschliesslich Terrorismus und dessen Finanzierung), Geldwäscherei und Korruption. Im Bereich der Wirtschaftskriminalität werden die Fälle von gesamtschweizerischer oder internationaler Ausprägung von der BA geahndet.[10] Für die koordinierte und einheitliche Bekämpfung der Cyberkriminalität auf operativer und strategischer Ebene wurde unter der Moderation der BA zusammen mit fedpol, unter Mitwirkung der kantonalen und nationalen Strafverfolgungsbehörden sowie Vertretenden der Prävention, die gemeinsame Plattform «Cyberboard» geschaffen (vgl. Kapitel 6.2.6).

Bundesamt für Polizei (fedpol): Die Kantone sind primär für die öffentliche Sicherheit zuständig. Das Bundesamt für Polizei übernimmt jedoch die Koordination, die Analyse und die Ermittlung in komplexen Fällen von Schwerstkriminalität und bei grenzüberschreitenden Themenbereichen wie der Internetkriminalität. Das neue Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) sieht explizit die Zusammenarbeit mit den Kantonen zur Bekämpfung von Cyberkriminalität vor.[11] fedpol fungiert auch als Verbindungsglied zum Ausland, denn Kriminalität macht keinen Halt vor Grenzen. Hinweise zur Prävention und Gefahren im Internet für die Bevölkerung werden regelmässig auf der Internetseite von fedpol publiziert.[12]

Sicherheitsverbund Schweiz (SVS): Der Delegierte für Bund und Kantone des Sicherheitsverbunds Schweiz fungiert als Partner für die Koordination der Umsetzung der Massnahmen der NCS (Schnittstelle zwischen Bund und Kantone) und dient als Ansprechstelle für die Cyber-Entwicklungen auf strategischer Ebene.

5.3 Einbezug der Kantone

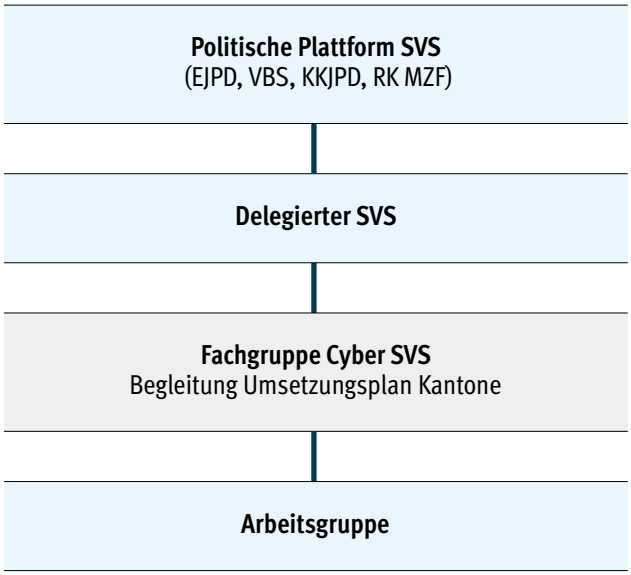

Abbildung 2: Organisation SVS[II]

Der Einbezug der Kantone kann sowohl auf der strategisch-politischen[13] als auch auf der operativen Ebene erfolgen.[14] Die vorliegende Abbildung zeigt die paritätischen Gremien des Sicherheitsverbundes Schweiz, in denen Vertretungen der Kantone Einsitz nehmen. Diese Organe behandeln sicherheitspolitische Herausforderungen, die sie gemeinsam betreffen, zu welchen auch die Cyberthematik gehört.

9 https://www.ncsc.admin.ch/ncsc/de/home.html (Stand: 21.01.2021).
10 https://www.bundesanwaltschaft.ch/mpc/de/home/die-bundesanwaltschaft/aufgaben-breit11.html (Stand: 04.01.2021).
11 Das Parlament verabschiedete das PMT-Gesetz (BBl 2020 7741) Ende September 2020.
12 https://www.fedpol.admin.ch (Stand: 07.01.2021).
13 Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) und die Regierungskonferenz Militär, Zivilschutz und Feuerwehr (RK MZF) sind vertreten.
14 Für ein konkretes Beispiel s. Anhang III.

5.4 Kantonale Cyber-Organisation

In einem Kanton sind grundsätzlich zwei Organisationsformen möglich:

- Eine verwaltungsinterne Person wird als Cyber-Koordinator/in, beispielsweise der Informationssicherheitsbeauftrage oder die Leiterin IT, designiert und agiert in den bestehenden Strukturen oder
- auf Beschluss der politischen Ebene wird eine Cyber-Organisation mit einer Cyber-Koordinatorin/ einem Cyber-Koordinator geschaffen, wie nachfolgend beispielhaft abgebildet ist.

Die Erhöhung der Cyber-Resilienz, respektive der integralen Sicherheit, in einem Kanton basiert auf einer optimalen Organisation der Verwaltung und ihren Partnern. Die vorliegende Abbildung dient als Beispiel und ist den Gegebenheiten des Kantons anzupassen.

5.4.1 Cyber-Koordinator/in

Der Mehrwert der Stelle einer Cyber-Koordinatorin/ einem Cyber-Koordinator liegt insbesondere in ihrer Funktion als Single Point of Contact (SPoC) innerhalb des Kantons, aber auch zu den Behörden auf der nationalen Ebene. Sie stellt zudem die Vernetzung zwischen den verschiedenen staatlichen und privaten Akteuren sicher. Bei einem Cyber-Vorfall obliegt ihr die Führung. Als Unterstützung kann die/der Cyber-Delegierte den Kantonalen Führungsstab (KFS)/ die Kantonale Krisenorganisation (KFO) beiziehen. Umgekehrt kann das «Operative Gremium» auch vom KFS/von der KFO bei einem Sicherheitsvorfall beigezogen werden. Bereits im Vorfeld sind deshalb die Zuständigkeiten festzulegen. Nachfolgend ist das Aufgabenportfolio des Cyber-Koordinators detailliert aufgeführt. Der Umfang der Wahrnehmung dieser Aufgaben erfordert personelle Ressourcen im geschätzten Umfang von einer Vollzeitstelle, die direkt einer oder mehreren Regierungsrätinnen oder Regierungsräten unterstellt ist. Zur Unterstützung der Cyber-Koordinatorin wird eine administrative Unterstützung empfohlen.

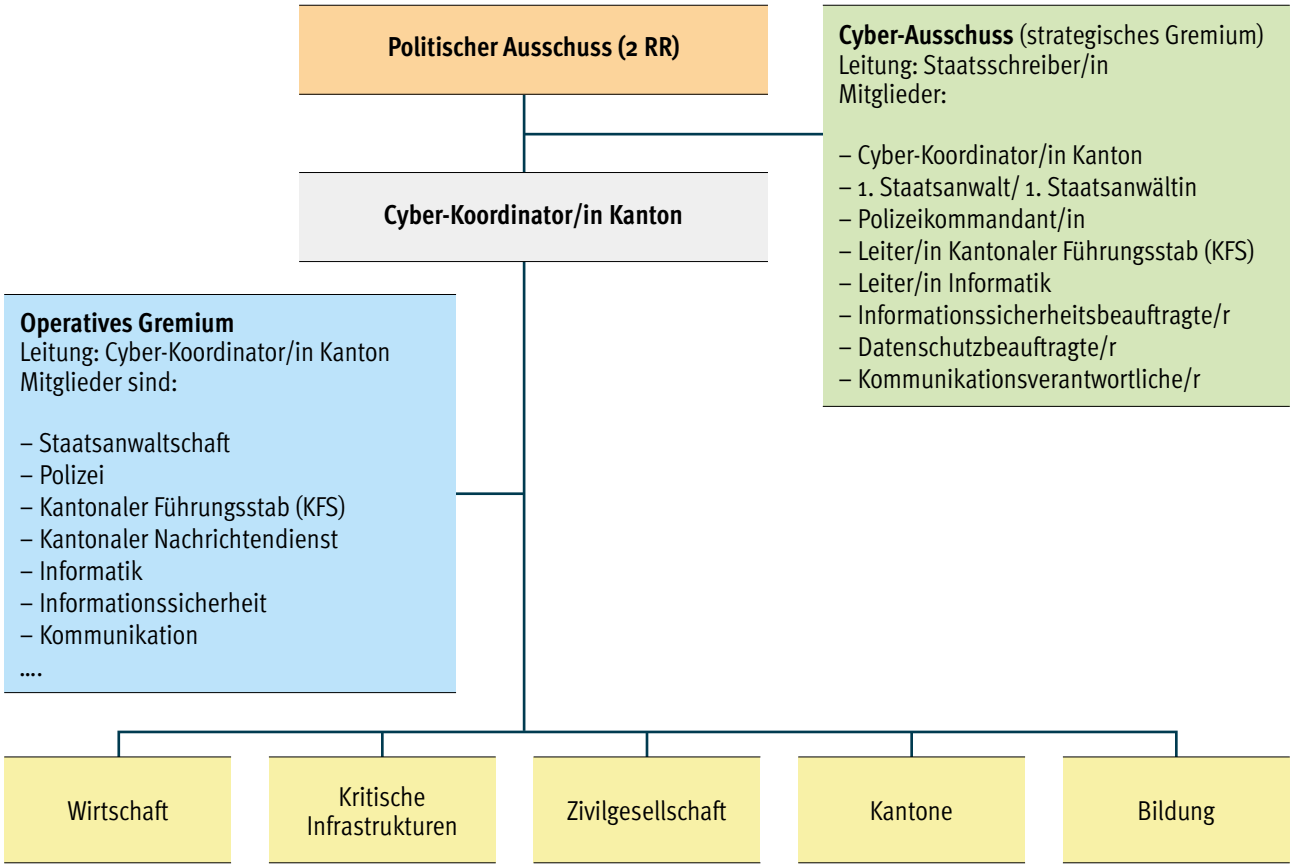

Abbildung 3: Kantonale Cyber-Organisation[III]

Aufgaben und Kompetenzen des Cyber-Koordinators (bei dieser Auflistung, die nicht abschliessend ist, handelt es sich um mögliche Aufgaben und Kompetenzen des Cyber-Koordinators):

	Nr.	Thema	HF[15]	M[16]
Dauerhaft		**Schaffung der kantonalen Organisationen für Cyber-Sicherheit**		**8**
	1	Verfolgt die Cyber-Entwicklung auf strategischer Ebene		
	2	Verfolgt die Cyberbedrohungslage Intern: Incident Management, Monitoring und kantonaler Nachrichtendienst Extern: OSINT, Meldungen von MELANI und vom Nachrichtendienst des Bundes	2	4
	3	Beurteilt das Sicherheitsdispositiv		
	4	Verantwortlich für das Risiko-Management (RM) und das Business Continuity Management (BCM)		
	5	Bildet die Schnittelle zum Delegierten des Bundes für Cyber-Sicherheit und zur Schweizerischen Informatikkonferenz (SIK), repräsentiert den Kanton in allen Cyber-Belangen		
	6	Erstellt Ausbildungsunterlagen und führt Schulungen durch Sensibilisiert die Verwaltung, Unternehmen und Bevölkerung	1	2
	7	Koordiniert die Umsetzung der Massnahmen der NCS im Kanton		
	8	Stellt Kontakte mit der Wirtschaft her, insbesondere mit den kantonalen kritischen Infrastrukturen		
	9	Stärkt die Resilienz der Verwaltung, Unternehmen und Bevölkerung	3	4
	10	Koordiniert die Übungen im Krisenstab mit den kantonalen kritischen Infrastrukturen	7	17
	11	Überprüft die Standardisierung / Regulierung bspw. Netzwerksicherheit	6	8
Situativ	12	Erstellt Anträge an die politische Ebene, bspw.: – Erstellt gesetzliche Vorgaben (Cyber-Gesetz oder Cyber-Verordnung) – Beantragt das Budget für die Umsetzung der Massnahmen zur Erhöhung der Cyber-Sicherheit – Beantragt die Umsetzung von Massnahmen		
	13	Beaufsichtigt Cybervorfälle, definiert Sofortmassnahmen und zieht Lehren aus dem Vorfall		
	14	Unterstützt auf Anfrage die Strafverfolgungsbehörden		
	15	Kann auf Anfrage die Strafverfolgungsbehörden eines anderen Kantons unterstützen		

15 Handlungsfeld aus dem Umsetzungsplan der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022
16 Massnahme aus dem Umsetzungsplan der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022

5.4.2 Politischer Ausschuss

Der Politische Ausschuss wird aus 2–3 Regierungsrätinnen/Regierungsräten gebildet.

Aufgaben:

- Definiert, welchem Departement die Cyber-Koordinatorin/ der Cyber-Koordinator unterstellt wird
- Schlägt dem Regierungsrat die Cyber-Koordinatorin/den Cyber-Koordinator und ihre/seine Stellvertretung zur Wahl vor
- Genehmigt die Ziele und prüft die jährliche Zielerreichung, den Jahresbericht, das Budget und das Einsatzkonzept

5.4.3 Cyber-Ausschuss

Das strategisch tätige Gremium wird von der Staatsschreiberin/ dem Staatsschreiber geleitet, welches sich aus den folgenden weiteren Mitgliedern zusammensetzt:

- Cyber-Koordinator/in
- 1. Staatsanwältin/1. Staatsanwalt vertritt die Staatsanwälte
- Polizeikommandant/in vertritt die Polizei, sie/er wird durch die Chefin/den Chef Lage und/oder die Chefin/den Chef Kriminalpolizei unterstützt
- Leiter/in KFS vertritt die Anforderung des Kantonalen Führungsstabes. Falls vorhanden wird sie/er durch die Chefin/den Chef Lage unterstützt
- Leiter/in Informatik vertritt die Interessen der IT-Leistungserbringenden
- der/die Informationssicherheitsbeauftragte
- der/die Datenschutzbeauftragte
- der/die Kommunikationsverantwortliche/r

Aufgaben:

- Genehmigt den Jahresbericht der Cyber-Koordinatorin/des Cyber-Koordinators
- Überprüft das operative Gremium mittels der definierten bzw. erreichten Ziele
- Beurteilt die Bewältigung von Cybervorfällen
- Beurteilt neue Angriffsvektoren, bspw. Internet of Things (IoT), Fahrzeuge der Blaulichtorganisationen
- Zieht Lehren aus den Cybervorfällen der eigenen Organisation oder der Umwelt
- Beurteilt den Ausbildungsstand des operativen Gremiums
- Der Cyber-Ausschuss definiert Rahmenbedingungen/Sicherheitsstandards für die KMUs
- ...

5.4.4 Operatives Gremium

Das operative Gremium wird von der Cyber-Koordinatorin/ vom Cyber-Koordinator geleitet. Einsitz in dieses Gremium nehmen die Vertretenden von den folgenden Stellen:

- Staatsanwaltschaft[17]
- Polizei
- Kantonaler Führungsstab
- Kantonaler Nachrichtendienst
- Informatik
- Informationssicherheit
- Vertretende kritischer Infrastrukturen

Aufgaben:

- Bewältigt Cybervorfälle
- Beurteilt die Cyberentwicklung in ihren Bereichen und deren Gegenmassnahmen
- Stellt sicher, dass die Mitarbeitenden ausgebildet und sensibilisiert sind

17 Die Staatsanwältin/der Staatsanwalt, die/der als SPoC im Cyber-Case von der Bundesanwaltschaft fungiert, sollte auch im Operativen Gremium Einsitz nehmen und vice versa.

– Stellt sicher, dass in ihrer Organisation die notwenigen Ressourcen (Mitarbeitende, Hard- und Software) vorhanden sind

– ...

5.5 Zusammenarbeit innerhalb der Kantone

Die Cyber-Koordinatorin/der Cyber-Koordinator arbeitet departemententsübergreifend und mit den Verantwortlichen der kritischen Infrastrukturen sowie weiteren Organisationen zusammen.

5.6 Zusammenarbeit zwischen den Kantonen

Die Cyber-Koordinatorin/der Cyber-Koordinator arbeitet mit den Cyber-Koordinatorinnen/Cyber-Koordinatoren der anderen Kantone zusammen.

5.7 Mindestanforderungen

Damit die Cyber-Organisation erfolgreich ist, müssen die nachfolgenden Voraussetzungen geschaffen werden. Allenfalls können sie auch vom Cyber-Koordinator/von der Cyber-Koordinatorin initiiert werden.

– Ausbildung- und Wissensvermittlung von kantonalen und kommunalen Behörden und Partnern

– Übersicht Geschäftsprozesse, Infrastruktur, Lieferanten und Dienstleistende: Die wichtigsten Geschäftsprozesse der kantonalen Verwaltung und die Prozesse der Partner sowie die Schnittstellen zu diesen müssen bekannt sein, um Sicherheitsvorkehrungen treffen zu können[18]

– Vorhandenes und geprüftes Business Continuity Management (BCM)

– Vorhandenes Risikomanagement

– Vorhandenes Informationssicherheitsmanagementsystem (ISMS)

– Definierte und dokumentierte Prozesse für die Bewältigung eines Cybervorfalls

18 Im Rahmen der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022 nehmen die Kantone mittels eines vom SVS entwickelten Tools eine Selbsteinschätzung ihrer Cyber-Risiken 2020 vor.

6. Cyber-Risiken und -Bedrohungen

Es gibt verschiedene Arten von Cyber-Risiken und -Bedrohungen. Exemplarisch sind nachfolgend jeweils zwei Typen von Gefahren beschrieben.

6.1 Cyber-Risiken

6.1.1 Ausfall IKT-Mittel

Das Bundesamt für Bevölkerungsschutz definiert den Ausfall von IKT-Mitteln wie folgt: «Von einem Ausfall der Informations- und Kommunikationstechnologien (IKT) wird dann gesprochen, wenn technische Mittel zur Verarbeitung oder Weiterleitung von Informationen temporär nicht mehr verfügbar sind. Wegen der verbreiteten Anwendung von IKT kann ein solcher Ausfall gravierende Konsequenzen haben. Das Schadensausmass ist abhängig von der Dauer, von der Art der betroffenen Technologien, der Anzahl und der Bedeutung der betroffenen Dienste und Nutzer sowie Beschädigung von Daten. Auch Ausfälle von spezifischen Systemen können zu grossen Schäden führen, wenn etwa die IKT basierten Kontrollsysteme von kritischen Infrastrukturen (Kraftwerke, Transportsysteme etc.) betroffen sind. Ein Ausfall von IKT kann deshalb zu verschiedenen weiteren Gefährdungen führen, weil viele Infrastrukturen von einer funktionierenden IKT abhängen und durch diese Technologien miteinander vernetzt sind. Ein Ausfall der IKT kann durch verschiedene Ereignisse ausgelöst werden. Beispiele dafür sind Störungen oder Ausfälle von Komponenten, menschliche Fehlhandlungen, Naturereignisse (z. B. Erdbeben), kriminelle Handlungen (Cybercrime, Cyberterror) oder technische Pannen (Stromausfall).»[19]

6.1.2 Auslagerung von IT-Leistungen

Daten können nicht nur auf eigenen Systemen verloren gehen oder gestohlen werden. Wenn (IT-) Dienstleistungen wie beispielsweise im Bereich der Wasserversorgung ausgelagert werden, geht oft ein Verlust an Kontrolle damit einher. Denn es ist unklar, welche Sicherheitsmassnahmen und Vorgehensweisen in der Vorfallbewältigung von den Zulieferern/Dienstleistern umgesetzt werden. Das Risiko erhöht sich, wenn mehrere Dienstleistungen extern erbracht werden; in diesem Fall trägt ein Kanton oder eine Gemeinde ein sogenanntes Klumpenrisiko. Die Melde- und Analysestelle Informationssicherung (MELANI) empfiehlt deshalb vertraglich festzuhalten, dass die Partner entsprechende Sicherheitsvorkehrungen treffen, auch wenn damit ein Kontrollaufwand einhergeht. [20]

6.2 Cyber-Bedrohungen

6.2.1 Cyber-Angriff

Ein Cyber-Angriff wird im Sicherheitspolitischen Bericht 2016 wie folgt definiert: «Beabsichtigte unerlaubte Handlung einer Person oder einer Gruppierung im Cyber-Raum, um die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen und Daten zu beeinträchtigen; dies kann je nach Art des Angriffs auch zu physischen Auswirkungen führen.»[21]

19 Bundesamt für Bevölkerungsschutz (2015). *Nationale Gefährdungsanalyse – Gefährdungsdossier Ausfall Informations- und Kommunikationstechnologien (IKT)*. https://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html#ui-collapse-952 (Stand: 07.11.2020).

20 NCSC (2019). *Halbjahresbericht 2019/1 (Januar – Juni)*, S. 32. https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte.html (Stand: 07.01.2021).

21 Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (2016). *SIPOL B 2016: Die Sicherheitspolitik der Schweiz Bericht des Bundesrates,* S. 7884. https://www.vbs.admin.ch/de/themen/sicherheitspolitik/sicherheitspolitische-berichte/sicherheitspolitischer-bericht-2016.detail.document.html/vbs-internet/de/documents/sicherheitspolitik/sipolb2016/SIPOL-B-2016-de.pdf.html (Stand: 16.10.2020).

6.2.2 Cyber-Kriminalität

Cyber-Kriminalität wird im Sicherheitspolitischen Bericht von 2016 folgendermassen definiert: «Gesamtheit aller strafbaren Handlungen und Unterlassungen im Cyber-Raum.»[22] Die frühe Doktrin[23] unterschied zwischen Cybercrime im engeren und im weiteren Sinne. Unter Cybercrime im engeren Sinne verstand man die sog. «Computertatbestände»; von Datenbeschaffung im Sinne von Art. 143 StGB bis betrügerischem Missbrauch einer Datenverarbeitungsanlage im Sinne von Art. 147 StGB. Cybercrime im weiteren Sinne fasste alle Delikte zusammen, wo der Computer Tat- oder Beweismittel ist. Diese Unterscheidung ist heute als überholt zu bezeichnen, zumal Cyberphänomene meist aus verschiedenen Delikten und einer Kombination der Tatbestände nach obiger Einreihung bestehen. Gemäss jüngerer Lehre [24] ist nach Komplexität des Phänomens und der zur Aufklärung nötigen Ermittlungshandlungen zu unterscheiden, nämlich:

1. Hightech-Crime bei internationalen Gruppierungen, welche grösstmöglich anonymisiert gewerbsmässige Delikte begehen. Die Aufklärung erfordert den gezielten Einsatz von geheimen Überwachungsmassnahmen in aufwändigen operativen Verfahren.

2. Cybercrime fasst klassische Erpressungs- und Betrugsformen zusammen, welche mit grossem Aufwand, aber ohne Einsatz von Echtzeitüberwachungsmassnahmen untersucht werden.

3. Schliesslich umfasst die Kategorie der digitalisierten Kriminalität sämtliche Delikte, wo ein EDV-Device oder Datenträger Tat- oder Beweismittel ist und die Ermittlung der Täterschaft mittels einfachen Rechtshilfemassnahmen oder Anschlussinhaberabfragen möglich ist. Cybercrime ist daher mehr Ermittlungsmethode zur Identifikation von Täterschaften im Inter- und Darknet als ein Deliktsfeld.

Für ein einheitliches Verständnis und zur justiziellen Koordination sind die am häufigsten auftretenden Phänomene zu definieren, wozu im Rahmen der NCS 2012–2017 die sog. Phänomenblätter entwickelt wurden. Der Katalog, der die verschiedenen Cyber-Phänomene enthält, kann von Behörden beim Bundesamt für Polizei bezogen werden.

22 Vgl. ebd.: S. 7884.
23 Allianz der schweizerischen Strafverfolgung zur Bekämpfung der Cyberkriminalität, Protokoll der 1. Sitzung vom 2. September 2016.
24 Staatsanwaltsakademie, Universität Luzern, Cybercrime Kurse I-III, Kompetenzzentrum Cyber-crime, Kanton Zürich.

6.2.3 Beurteilungsfaktoren

Für die Beurteilung eines Ereignisses müssen die folgenden Aspekte[25] zwingend berücksichtigt werden, die voneinander abhängig sind.

Gefahrenquelle	– Merkmale der Täterschaft (Ideologie, Gewaltbereitschaft, Fähigkeit und Know-how, Organisationsgrad, Ressourcen, kontrollierte / bereits verfügbare Infrastruktur) – Verhalten eines Staates oder im Land ansässiger Organisationen (krimineller oder parastaatlicher Natur) – Verletzlichkeit von Systemen (Härtung, Schutzmassnahmen, Schnittstellen/ Zugangspunkte, Social Engineering, fehlende Eingliederung der Informationssicherheit in integrale, strategische Sicherungsprozesse)
Zeitpunkt	– In der Regel abhängig von betrieblichen, politischen und/oder gesellschaftlichen Entscheiden und Entwicklungen – Der Aufbau der relevanten Mittel und Infrastruktur kann bereits in einem anderen Zusammenhang erfolgt sein. – Die widerrechtliche Manipulation eines IT-Systems kann zeitlich früher erfolgen als der eigentliche Cyber-Angriff, der unter Umständen nur sehr kurz ist
Ort und Ausdehnung	– Grösse und relevante Merkmale des Angriffsobjektes (Einzelobjekt, Branche, Sektor bzw. Vernetzung der Sektoren, spezifische Technologie etc.) – Quelle des Angriffs (Ort, wo sich die Urheber und die Mitwirker des Angriffs befinden) – Verwendete Infrastrukturen (Netzwerke, Schnittstellen, Protokolle etc.)
Ereignisablauf	– Vorwarnzeit des Ausfalls – Wirkung der präventiven Schutzmassnahmen, inkl. Rechtspraxis – Wirkung der spezifisch ergriffenen Gegenmassnahmen – Ablauf des Angriffs (ggf. in Eskalationsstufen) – Verhalten von betroffenen Organisationen, Einsatzkräften und verantwortlichen Behörden – Reaktion der Bevölkerung und der Politik

25 BABS (2015). *Nationale Gefährdungsanalyse – Gefährdungsdossier Cyber-Angriff.* https://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html#ui-collapse-938 (Stand vom 07.01.2021).

6.2.4 Angreifergruppen

Die vorliegende Tabelle illustriert die Wahrscheinlichkeit und die Professionalität von Angriffen im virtuellen Raum auf Personen, Firmen, Banken, kritische Infrastrukturen, Polizei, Sanität, Feuerwehr, Spitäler etc.) und öffentliche Organe.

Der blaue Pfeil bildet die Professionalität der Angreifer ab. Der graue Pfeil zeigt wie hoch die Wahrscheinlichkeit eines Angriffs ist.

Lesebeispiel: Die Angreifer «Staatliche Akteure» verfügen über sehr viel Wissen und finanzielle Mittel um gezielte Angriffe zu lancieren und zwar mit einem definierten Auftrag. Die Wahrscheinlichkeit, dass dieser Fall eintritt, ist allerdings gering. Hingegen ist es sehr viel wahrscheinlicher, dass Vandalen mit minimalsten Mitteln einen Angriff lancieren.

	Angreifer	Wissen	Ziele	Mittel	Vorgehen	Wahrscheinlichkeit
Gezielt	– Staatliche Akteure – Geheimdienste	Sehr hoch	– Information – Spionage – Bekämpfung – Terrorismus/ Kriminalität – Schaden	– Grosse finanzielle Möglichkeiten – Fokus auf Nutzen weniger auf Kosten	– Kaufen Know-how ein und bilden Spezialisten aus – Unauffällige und nachhaltige Angriffe	Sehr gering
	Terroristen	hoch	– Schaden – Aufmerksamkeit – Manipulation, Beeinflussung der Politik	– Mittlere finanzielle Mittel, damit ein Angriff erfolgreich ausgeführt werden kann	– Kaufen Know-how auf dem Schwarzmarkt ein – Angriff physisch und logisch	Gering
	(Organisierte) Kriminalität	Mittel		– Business – Langfristig Geld verdienen – Kosten und Nutzen müssen stimmen	– Bestehende Banden – Spontane organisierte Banden von Spezialisten – Bestechung	Mittel
Opurtunistisch	Hacktivist, Gruppen	Gering	– Aufmerksamkeit – Schaden – Anprangern der Verletzlichkeit von Systemen	– Minimale Mittel – Grosse Reichweite	– Hoch motivierte Amateure und Spezialisten – Entwicklen unvorhergesehene Eigeninitiative	Hoch
	Vandalen, Script Kiddies	Sehr gering	Ruhm und Ansehen	– Minimale Mittel – Minimales Wissen	Einsatz von verfügbaren Tools	Sehr hoch

Abbildung 4: Angreifergruppen[IV]

6.2.5 Auswirkungsdiagramm

Dargestellt sind Ereignisse und Entwicklungen aus dem «Katalog möglicher Gefährdungen» des Bundesamts für Bevölkerungsschutz[26], die Auslöser oder Folge eines Ausfalls der IKT-Infrastruktur sein können: Die Erbringung von Dienstleistungen kann leicht beeinträchtigt bis verunmöglicht werden; der Geschäftsbetrieb kann kurz- bis langfristig gestört werden; ein Imageverlust, allenfalls sogar ein internationaler, kann in der Folge entstehen.

Wie in dieser Grafik ersichtlich ist, ist die Wirtschaft stark von Cyberkriminalität betroffen. Weltweit resultiert ein Verlust von 600 Milliarden Dollar für die Wirtschaft. [27] Die globale Umfrage zur Wirtschaftskriminalität 2018 von PricewaterhouseCoopers hat ergeben[28], dass Cyberkriminalität das am zweit häufigste Wirtschaftsdelikt in der Schweiz ist (44 %, 31 % weltweit). Entsprechend hoch ist auch der entstandene Schaden für die Schweiz. Die häufigsten Angriffstechniken waren Phishing (42 %) und Malware (31 %). Dabei verfügen nur gerade 54 Prozent der Schweizer Firmen über ein einsatzbereites Cybersecurity-Programm. Cyberkriminalität wird auch in Zukunft als das bedeutendste Risiko wahrgenommen. Deshalb wird Cybersecurity zur Priorität der Geschäftsführung und entsprechende Anstrengungen sind zu unternehmen.

Innerhalb der Kategorie Cyber-Angriff wird als Beispiel die vorsätzliche Handlung beschrieben, unter

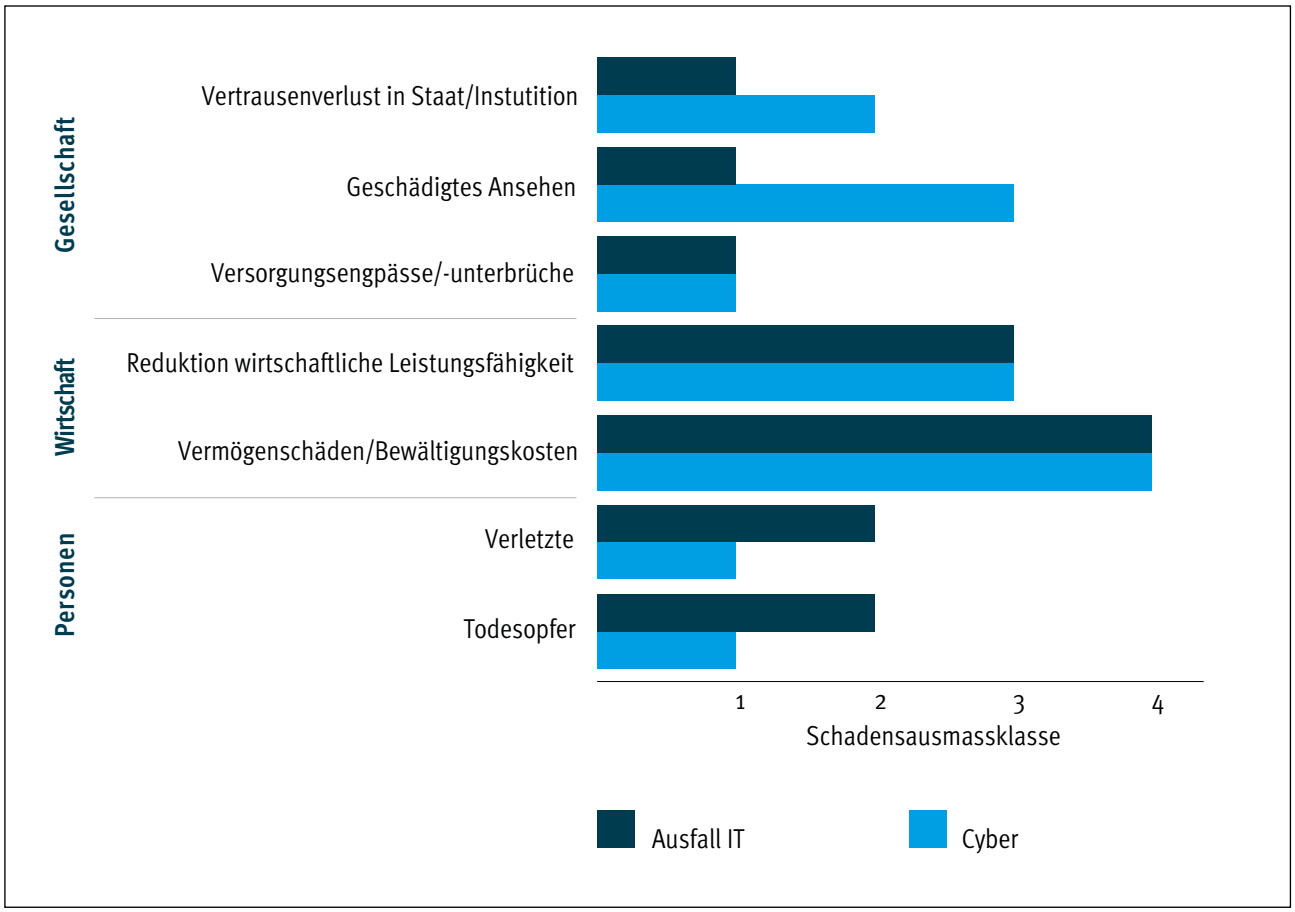

Abbildung 5: Auswirkungsdiagramm[v]

26 Bundesamt für Bevölkerungsschutz (2013). *Katalog möglicher Gefährdungen. Grundlage für Gefährdungsanalysen.* http://www.alexandria.admin.ch/bv001492631.pdf (Stand: 15.10.2020).

27 McAfee (2018). *Economic Impact of Cybercrime— No Slowing Down.* https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf (Stand: 08.07.2020).

28 PricewaterhouseCoopers (2018). *Globale Umfrage zur Wirtschaftskriminalität 2018 – Schweizer Erkenntnisse.* https://www.pwc.ch/de/publications/2018/globale-umfrage-zur-wirtschaftskriminalitaet-2018.pdf (Stand: 12.10.2020).

welcher folgende Delikte zu verstehen sind: Sabotage gegen Gebäude, Räume und IKT-Mittel; Diebstahl und Weitergabe von Informationen oder IKT-Mitteln; Angreifer versuchen Malware in die IKT-Landschaft zu platzieren sowie die Ausnutzung von Sicherheitslücken in Betriebssystemen und Software. Daraus resultieren folgende Auswirkungen: Verminderung oder Verunmöglichung von Leistungen; Unberechtigte erhalten Zugang zu Gebäuden, Räumen, Daten, Informationen und IKT-Mitteln; Diebstahl von Werten und Informationen.

Mittels der vorliegenden Darstellung kann der Risikowert des vorliegenden Beispiels ermittelt werden, die die Auswirkung einer Eintretenswahrscheinlichkeit eines Ereignisses und den maximal zu erwartenden Schaden aufzeigt.

Der Schaden wird mittels drei Bereiche beurteilt:

- finanzieller Schaden;
- Ausfall von kritischen Geschäftsprozessen;
- Ausfall von nichtkritischen Geschäftsprozessen.

In unserem Beispiel wurde der Bereich «Ausfall von kritischen Geschäftsprozessen» als prioritär beurteilt und erhält daher den Wert 4. Die Eintretenswahrscheinlichkeit wurde mit «Wahrscheinlich» bewertet, was einem Wert von 5 entspricht. In diesem Beispiel beträgt der Risikowert (der Risikowert bildet das Produkt aus Eintretenswahrscheinlichkeit mal maximaler Schaden) somit 20.

Ein umfassendes Risikomanagement ist unabdingbar, um Cyber-Angriffe und die daraus resultierenden Folgen bewältigen zu können.

	Auswirkungen			Risikowert = Auswirkung x Eintretenswahrscheinlichkeit					
Stufe	**Finanzielle Auswirkungen in Mio. CHF**	**Ausfall von kritischen Geschäftsprozessen in Tagen**	**Ausfall von nicht kritischen Geschäftsprozessen in Tagen**						
sehr hoch **6**	› 10	**›14**		6	12	18	24	30	36
hoch **5**	1 bis 10	**7 bis 14**		5	10	15	20	25	30
wesentlich **4**	0.5 bis 1	**3 bis 7**		4	8	12	**16**	**20**	24
moderat **3**	0.1 bis 0.5	**0.5 bis 3**	**›3**	3	6	9	**12**	15	18
gering **2**	**0.01 bis 0.1**	**0.5**	1 bis 3	2	4	6	8	10	12
sehr gering **1**	‹ 0.01		‹ 1	1	2	3	4	5	6
				sehr unwahrscheinlich **1** **über 10 Jahre**	unwahrscheinlich **2** **alle 5 bis 10 Jahre**	selten **3** **alle 3 bis 5 Jahre**	möglich **4** **alle 2 bis 3 Jahre**	wahrscheinlich **5** **alle 1 bis 2 Jahre**	sehr wahrscheinlich **6** **Mehrmals pro Jahr**
				Eintretenswahrscheinlichkeit					

Abbildung 6: Risikomatrix[VI]

Lesebeispiel

Schritt 1	Beurteilung des finanziellen Risikos	Beurteilung der Ausfälle von Geschäftsprozessen			
	Der finanzielle Schaden liegt zwischen 0.01 und 01.1 Mio. CHF. Stufe 2				
Schritt 2		Die maximale Ausfalldauer von kritischen Geschäftsprozessen wird beurteilt			
		Der Ausfall von kritischen Geschäftsprozessen darf maximal 7 Tage dauern. **Stufe 4**			
Schritt 3			Die maximale Ausfalldauer von nicht kritischen Geschäftsprozessen wird beurteilt		
			Der Ausfall von nicht kritsichen Geschäftsprozessen darf über 3 Tage dauern. Stufe 3		
Es wird die maximale Stufe der Auswirkung angewendet. In diesem Beispiel beträgt der Wert **4**					

Schritt 4		**Es wird die Eintretenswahrscheinlichkeit beurteilt**
		Der Ausfall findet alle 1 bis 2 Jahre statt. **Stufe 5**
	Der Risikowert (Auswirkungen (4) x Eintretenswahrscheinlichkeit (5) = **20**	

Schritt 5	Umsetzung der risikomindernden Massnahmen	Da der Risikowert **20** beträgt, müssen die risikomindernden Massnahmen innert 1 Monat umgesetzt werden.		Grundschutz Werte 1 bis 4	Es müssen keine risikomindernden Massnahmen umgesetzt werden.
				Erhöhter Schutzbedarf Werte 5 bis 15	Es müssen risikomindernde Massnahmen innert 6 Monaten umgesetzt werden.
				Sehr hoher Schutzbedarf Werte 18 bis 36	Es müssen risikomindernde Massnahmen innert 1 Monat umgesetzt werden.

Quelle: Gemäss Vorgaben Informatiksteuerungsorgan des Bundes
P042 – Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) – Version 4.3

6.2.6 Bekämpfung von Cyber-Kriminalität

Die Bekämpfung der Cyberkriminalität ist eine klassische Verbundsaufgabe der Strafverfolgungsbehörden von Bund und den Kantonen. Aus diesem Grund wurde das «Konzept Cyberboard» 2018 erstellt. Das Cyberboard ermöglicht die notwendige verstärkte Koordination im Rahmen der Verbundsaufgabe bei der Bearbeitung von interkantonalen und internationalen Fällen. Das Cyberboard fungiert als Plattform, die auf der Beibehaltung der bisherigen Strukturen und Kompetenzen basiert. Es gibt keine Zuständigkeitsänderungen und es werden keine neuen Behörden kreiert. Das Cyberboard ist in eine operative und in eine strategische Ebene unterteilt: Cyber-CASE, Cyber-STATE und Cyber-CORE arbeiten operativ, Cyber-STRAT strategisch.

- **Cyber-STRAT:** ist verantwortlich für die strategische Steuerung und Ausrichtung des operativen Bereichs des Cyberboards.
- **Cyber-CORE:** Dieses Gremium ist die Drehscheibe des operativen Bereichs des Cyberboards. Gewisse Aufgaben von Cyber-CORE werden bisher durch Mitarbeitende der BA wahrgenommen; das Gremium an sich wurde bis anhin jedoch nicht institutionalisiert.
- **Cyber-CASE:** Nationale Fallübersicht, Erfahrungen austauschen unter Kantonen/Behörden, Besprechung aktueller Fälle etc.
- **Cyber-STATE:** national konsolidierte Lagebildbeurteilung sicherstellen (anstatt nur im Kanton). Bis anhin wurde auch Cyber-STATE bewusst nicht institutionalisiert, weil MELANI als zentraler Inputgeber für die Lage in Cyber-CASE vertreten ist.

Cyberboard

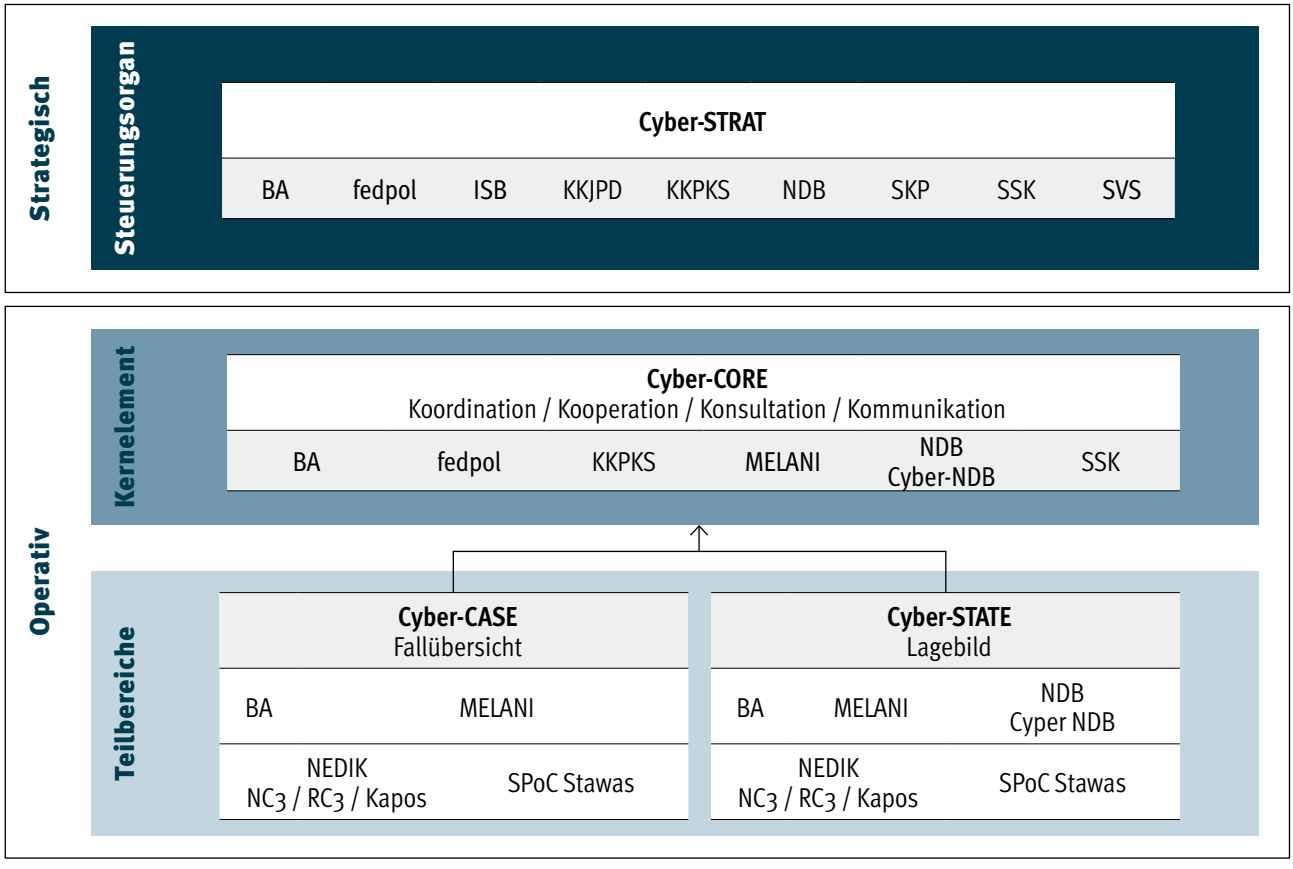

Abbildung 7: Cyberboard[VII]

7. Strategien und Standards

Dieses Konzept basiert auf den nachfolgenden Strategien und Standards, die mitunter explizit die Erstellung des vorliegenden Konzepts für die kantonale Cyber-Organisation und dessen Umsetzung vorsehen. Durch die Anwendung von Standards wird zudem sichergestellt, dass geeignete Kontrollen möglich sind.

7.1 Grundlagendokumente auf Stufe Bund

- Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) 2018–2022[29]
- Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) 2018–2022[30]
- Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung 27.05.2020[31]
- Umsetzungsplan zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022[32]
- Minimalstandard zur Verbesserung der IKT-Resilienz 2018[33]
- Risiko- und Verwundbarkeitsanalyse und Resilienz-Massnahmen PRJV 2018[34]

7.2 Grundlagedokumente auf Stufe Kanton

- Cybersecurity Core Framework/ NIST Standard 2018[35]
- Netzwerk-Sicherheitspolitik (NSP) 2017[36]
- Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022[37]
- Leitlinien der Kantone zur Digitalen Verwaltung 2018[38]
- Strategien/Dokumente des Kantons [39]

29 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-70482.html (Stand: 07.01.2021).
30 https://www.babs.admin.ch/de/aufgabenbabs/ski/nationalestrategie.html (Stand: 15.07.2020).
31 https://www.admin.ch/opc/de/official-compilation/2020/2107.pdf (Stand: 15.07.2020).
32 https://www.ncsc.admin.ch/ncsc/de/home/strategie/umsetzungsplan.html (Stand: 07.01.2021).
33 https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html (Stand: 15.07.2020).
34 Diese Dokumente können auf Anfrage beim Bundesamt für Bevölkerungsschutz bezogen werden.
35 National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Stand: 05.11.2020).
36 Schweizerische Informatikkonferenz: https://intranet.sik.ch/dokumentation/ITEmpfehlungen/ITEmpfehlungen/Forms/AllItems.aspx?RootFolder=%2Fdokumentation%2FITEmpfehlungen%2FITEmpfehlungen%2FNSP%20Network%20Security%20Policies&FolderCTID=0x0120004325A2A049A4D545B893CFF7CD3EC2F9&View=%7b9FD8BBC0-634A-4D17-B788-1D3F75D21ABD%7d (Stand: 14.10.2020).
37 https://www.svs.admin.ch/de/themen-/cybersicherheit/cybersicherheit-kantone.html (Stand: 14.10.2020).
38 https://kdk.ch/uploads/media/Leitlinien-E-Government_20180927.pdf (Stand: 09.07.2020).
39 Bei diesen Angaben handelt es sich um Beispiele. Ergänzungen sind mit den gesetzlichen Grundlagen des jeweiligen Kantons vorzunehmen.

8. Rechtliche und sonstige Vorgaben

Dieses Konzept stützt sich auf die folgenden rechtlichen Grundlagen oder Vorgaben[40]:

Diese Vorgaben sind regelmässig zu überprüfen, d.h. circa einmal pro Jahr; je nach Ergebnis sind entsprechende Anpassungen in der Organisation erforderlich.

Kurzbezeichnungen der Gesetze oder Verordnungen	Gesetz	Verordnung	Weisung	Andere Vorgabe	Name	Datum Inkrafttreten
VOG	X				Verwaltungsorganisationsgesetz	12.01.2007
VKKO		X			Verordnung kantonale Krisenorganisation	05.09.2018
CyRV		X			Cyberrisikenverordnung	27.05.2020
W-SVI			X		Sicherstellung der Verfügbarkeit der Informatikmittel	03.05.2004
BVI				X	Vorgaben für die Materialbeschaffung von Informatikmitteln	02.06.2015

40 Diese Grundlagen oder Vorgaben können ergänzt und/oder verändert werden, um die jeweilige kantonale Cyber-Organisation aufzubauen.

9. Ausgangslage

9.1 Parlamentarische Vorstösse im Bereich Cybervorsorge

Parlamentarische Vorstösse bilden eine wichtige Grundlage für die Umsetzung der Cyber-Organisation im Kanton. Die vorliegende Tabelle dient als Vorlage zur Übersicht der jeweiligen kantonalen Vorstösse. Beim aufgeführten Eintrag handelt es sich um ein Musterbeispiel.

Geschäftsnummer	Datum	Titel	Name	Art	Status – Auftrag – in Bearbeitung – Erledigt
16.5128	12.02.2020	Cyber-Kriminalität	Marina Muster	Interpellation	In Bearbeitung

9.2 Vorfälle

Die Auflistung der Vorfälle (im Kanton) ermöglicht eine systematische Darstellung und Übersicht der Angriffe, die unterschiedlich schwere Schäden und hohe Kosten zur Folge hatten bzw. noch immer haben können, wie folgende Beispiele verdeutlichen.

Datum	Titel	Beschreibung	Geschätzte Gesamtkosten
12.06.2019	Ransomware	Verschlüsselung von Informationen	200‘000 CHF
25.09.2019	Datenabfluss	Es sind Daten aus dem Departement x abgeflossen	1‘000‘000 CHF
15.09.2019	Berechtigungen	Durch Unberechtigte benutzte admin. Rechte	30‘000 CHF

Cyber-Sicherheit ist essentiell um solche Vorfälle zu verhindern; die Schaffung der kantonalen Cyber-Organisation leistet einen entsprechenden Beitrag dazu.

9.3 Umgesetzte Organisations-, IT- und Informationssicherheitsmassnahmen

Die vorliegende Darstellung illustriert beispielhaft die Umsetzung von Massnahmen eines Kantons. Diese Tabelle dient als Überblick und als Grundlage für die Beurteilung der Cyber-Resilienz. Sie ist laufend anzupassen.

Thema	Umsetzungsgrad
Inkraftsetzung der Informationssicherheitsweisung des jeweiligen Kantons	100%
Umsetzung der Massnahmen zum Schutz der Verwaltung	50%
Umsetzung der Massnahmen zum Grundschutz und erhöhten Schutz der IKT-Mittel	75%
Umsetzung der Netzwerksicherheit (Konzept, Realisierung und Prüfung)	80%
Umsetzung Business Continuity Management (BCM) inkl. Risiko- und Notfallmanagement	70%
Szenarien Cyber und IT-Notfall in der kantonalen Krisenorganisation	20%

9.4 Das Business Continuity Management (BCM) und die IT-Notfallvorsorge

Das Business Continuity Management (BCM) und die IT-Notfallvorsorge sind ein wichtiger Bestandteil bei der Bewältigung eines Cyber-Angriffs. Das BCM sollte in der Verwaltung aufgebaut und geprüft sein und durch die IT (im Rahmen des IT-Service Continuity Management) unterstützt werden.

9.5 Integrale Betrachtung

Die folgenden Elemente können Einfluss auf das Informationssicherheitssystem haben:

- Kantonale Verwaltung
- Bevölkerung
- Kritische Infrastrukturen (KIs)
- Gebäude und Räume
- Informations- und Kommunikationsmittel (IKT) und Informationen (bspw. Datenbanken)
- Interne und externe Dienstleistende und Lieferanten
- Nationale Anlaufstelle (NCSC)

Diese Angaben ermöglichen die Erstellung eines umfassenden Lagebildes. Aus den daraus gewonnen Erkenntnissen können Risiken und risikomindernde (Sofort-)Massnahmen abgeleitet werden.

10. Anhänge

I. Empfohlene Standards

Der Kanton sollte einen der folgenden Standards für seine Informations-, respektive Cybersicherheit, festlegen.

Norm oder Empfehlung	Titel
ISO/IEC 27001	Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen
ISO/IEC 27002	Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmassnahmen
ISOI/EC 31000	Risikomanagement
ISO/IEC 22301	Betriebskontinuitätsmanagement
BSI-Standards	Empfehlung des deutschen Bundesamtes für Sicherheit in der Informationstechnik
NIST 800-82	Standard für die Informationssicherheit wird im IKT-Minimalstandard vom Bundesamt für wirtschaftliche Landesversorgung (BWL) aufgeführt.

II. Referenzierte Dokumente

Die zu referenzierenden Dokumente sind jeweils vom Kanton anzupassen.

Nr.	Titel	Autor	Datum/Version
[1]	Nationale Strategie zum Schutz vor Cyberrisiken (NCS) 2018–2022	Bundesrat	
[2]	Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) 2018	Bundesrat	
[3]	Umsetzungsplan der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022	Bundesrat	
[4]	Cyber-Strategie Kanton «Kantonsname»	Kantonsname	
[5]	Netzwerk-Sicherheitspolitik (NSP) 2017		
[6]	Weitere Dokumente des Kantons		
[7]	Weitere Dokumente des Kantons		
[8]	Weitere Dokumente des Kantons		

III. Beispiele von Cyber-Vorfällen

Beispiel 1: Stadtverwaltung Bern

Im Halbjahresbericht 2019/1 (Januar – Juni)[41] hält die Melde- und Analysestelle Informationssicherung (MELANI) bzw. der ICT-Sicherheitsbeauftragte der Stadt Bern, Martin Müller, fest, dass Schadsoftware wie Verschlüsselungs-Trojaner grosse Cybergefahren für Behörden und Unternehmen darstellen. Die Angreifer stellen Lösegeldforderungen und im Gegenzug versprechen sie, die Entschlüsselung der gesperrten Daten. Eine solche Garantie gibt es jedoch nicht. Die Stadtverwaltung Bern war in den Jahren 2017 und 2019 von solchen Attacken betroffen. Beunruhigend ist zudem der Umstand, dass solche Angriffe heute mit sehr wenig Wissen und Mitteln ausgeführt werden können. Technische Sicherheitsvorkehrungen wie Firewalls und ein Backup-Management sind deshalb zentral. Müller hält aber fest, dass die Schulung und Sensibilisierung der Mitarbeitenden die wichtigste Massnahme ist um die IKT-Sicherheit zu gewährleisten.

Beispiel 2: Postfinance

Anfang Dezember 2010 hat die Postfinance das Konto von Wikileak-Gründer Julian Assange gesperrt wegen falschen Angaben zu seinem Wohnort bei der Kontoeröffnung. Julian Assange hatte Genf angegeben, was sich bei der Überprüfung der Daten als falsch herausstellte. Als Reaktion von seinen Anhängern folgten gezielte Hacker-Angriffe, mit denen sie die Webseite der Postfinance während mehreren Stunden lahmlegten.[42]

Beispiel 3: Spital Wetzikon

Das Spital Wetzikon wurde im Oktober 2019 von einem sehr aggressiven Trojaner angegriffen. Der Angriff erfolgte mittels einer E-Mail, die äusserst authentisch der internen Kommunikation nachgestaltet wurde. Der Empfänger wurde aufgefordert, den Anhang, ein Word-Dokument, zu öffnen und ein Makro zu aktivieren. Der Angreifer verschaffte sich auf diese Weise Zutritt zum System und der Betroffene merkt nichts davon. Eine solche Attacke läuft in mehreren Phasen ab mit dem Ziel, möglichst viele Systeme zu identifizieren und Backups sowie Online-Systeme zu verschlüsseln. Dann folgt die Forderung nach Lösegeld, damit der Geschädigte wieder Zugriff auf seine Daten erhält. Das Spital Wetzikon hatte jedoch Glück und ein IT-Mitarbeiter entdeckte rechtzeitig Unregelmässigkeiten an der Firewall. So kam es nur zu Teilausfällen, denn die Angriffe konnten blockiert und Schäden bereinigt werden. Bei vielen Spitälern könnte die Sache allerdings schlimm enden. Denn viele Einrichtungen im Schweizer Gesundheitswesen erfüllen die Minimalstandards der IT-Sicherheit nicht.[43]

---

41 NCSC. *Halbjahresbericht 2019/1 (Januar – Juni)*, S, 5. https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte.html (Stand: 07.01.2021).

42 SDA (2010). «Postfinance-Webseite lahmgelegt», in: *Neue Zürcher Zeitung* vom 8. Oktober 2010, https://www.nzz.ch/postfinance-website_lahmgelegt-1.8594103?reduced=true (Stand: 12.01.2021).

43 Jenni, Thier (2020). «Wir hatten ein Riesenglück.» Das Spital Wetzikon wurde von einem Trojaner angegriffen – viele Krankenhäuser unterschätzen die Gefahr», in: *Neue Zürcher Zeitung* vom 28.01.2020, https://www.nzz.ch/digital/wir-hatten-ein-riesenglueck-ld.1536678?reduced=true (Stand: 07.01.2021).

Abbildungsverzeichnis

I Quelle: NCSC
II Quelle: SVS
III Quelle: SVS
IV Swisscom AG (2015). *Cyber Security: Die aktuelle Bedrohungslage und ihre Entwicklung.* https://www.swisscom.ch/content/dam/swisscom/de/about/unternehmen/portraet/netz/sicherheit/documents/cyber-security-report-2015.pdf.res/cyber-security-report-2015.pdf (Stand: 18.08.2020).
V BABS (2015). *Nationale Gefährdungsanalyse – Gefährdungsdossier Ausfall Informations- und Kommunikationstechnologien (IKT).* https://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html#ui-collapse-938n (Stand: 18.08.2020).
VI Darstellung: SVS
VII Quelle: Bundesanwaltschaft

Sicherheitsverbund Schweiz SVS
Tel. +41 58 462 20 29, www.svs.admin.ch

80.252.d 11.20