Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Energie BFE
Digital Innovation Office

Bericht vom 28 Juni 2021

Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung

Datum: 28 Juni 2021

Ort: Bern

Auftraggeberin:

Bundesamt für Energie BFE
CH-3003 Bern
www.bfe.admin.ch

Auftragnehmer/in:

Deloitte AG
General-Guisan-Quai 38, CH-8022 Zürich
www.deloitte.com/ch

BFE-Projektleitung:

Dr. Matthias Galus	Leiter Digital Innovation Office	matthias.galus@bfe.admin.ch

BFE-Begleitgruppe:

Dr. Fabian Heymann	Digital Innovation Office	fabian.heymann@bfe.admin.ch
Stephane Henry	Sektion Risiko und Rohrleitungen	stephane.henry@bfe.admin.ch

BFE-Vertragsnummer: SI/600481-01

Für den Inhalt und die Schlussfolgerungen sind ausschliesslich die Autoren dieses Berichts verantwortlich.

Bundesamt für Energie BFE
Pulverstrasse 13, CH-3063 Ittigen; Postadresse: Bundesamt für Energie BFE, CH-3003 Bern
Tel. +41 58 462 56 11 · Fax +41 58 463 25 00 · contact@bfe.admin.ch · www.bfe.admin.ch

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACER	Agency for the Cooperation of Energy Regulators
AI	Articifical Intelligence
AkkBV	Schweizerische Akkreditierungs- und Bezeichnungsverordnung
APT	Advanced Persistent Threat
BABS	Bundesamt für Bevölkerungsschutz
BAG	Bundesamt für Gesundheit
BAKOM	Bundesamt für Kommunikation
BAV	Bundesamt für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BCMS	Business Continuity Management Systems
BFE	Bundesamt für Energie
BSI	Deutsches Bundesamt für Sicherheit in der Informationstechnik
BWL	Bundesamt für die wirtschaftliche Landesversorgung
DAkkS	Deutsche Akkreditierungsstelle
DSG	Datenschutzgesetz
CDC	Cyber Defense Center
CER	Critical Entities Resilience
CERT	Computer Emergency Response Team
CDC	Cyber Defense Center
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CyRV	Cyberrisikenverordnung
DAkkS	Deutsche Akkreditierungsstelle
DIN	Deutsches Institut für Normung
EBV	Eisenbahnverordnung
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFD	Eidgenössisches Finanzdepartement
EGC	European Government CERTs Group
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ElCom	Eidgenössische Elektrizitätskommission
EnG	Energiegesetz
ENISA	Agentur der Europäischen Union für Cybersicherheit
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat
ENTSO-E	European Network of Transmission System Operators for Electricity
EnV	Energieverordnung
EnWG	Deutsches Energiewirtschaftsgesetz
ESTI	Eidgenössischen Starkstrominspektorat
EU	Europäische Union
EUDE	European Distribution System Operators
FINMA	Eidgenössischen Finanzmarktaufsicht
FINMAG	Finanzmarktaufsichtsgesetz

FIRST	Forum of Incident Response and Security Teams
FMG	Fernmeldegesetzt
GovCERT	Nationales Computer Emergency Response Team
ICS	Industrial Control System
IEC	Internationale Elektrotechnische Kommission
IKT	Informations- und Kommunikationstechnologien
IoT	Internet of Things
ISMS	Informationssicherheits-Managementsystem
ISO	Internationale Organisation für Normung
IT	Information Technology
KEG	Kernenergiegesetz
KI	Kritische Infrastruktur
LVG	Landesversorgungsgesetz
MELANI	Melde- und Analysestelle Informationssicherung
MELANI OIC	Melde- und Analysestelle Informationssicherung Operation Information Center
METAS	Eidgenössischen Institut für Metrologie
NCS	Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken
NCSC	Nationales Zentrum für Cyber-Sicherheit
NEDIK	Netzwerk Ermittlungsunterstüt-zung digitale Kriminalitätsbekämpfung
NERC	North American Electric Reliability Corporation
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIS-Richtlinie	Richtlinie über die Sicherheit von Netz- und Informationssystemen
NIST	National Institute of Standards and Technology
OSINT	Open Source Intelligence
OT	Operational Technology
SAS	Schweizerische Akkreditierungsstelle
SCADA	Supervisory Control and Data Acquisition System
SIEM	Security Information and Event Management
SKI	Nationale Strategie zum Schutz Kritischer Infrastrukturen
SOAR	Security Orchestration and Automated Response
SOC	Security Operations Center
SPoC	Single Point of Contact
StromVG	Stromversorgungsgesetz
StromVV	Stromversorgungsverordnung
ÜNB	Übertragungsnetzbetreiber
USA	Vereinigten Staaten von Amerika
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VNB	Verteilnetzbetreiber
VSE	Verband Schweizerischer Elektrizitätsunternehmen
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung

Executive Summary (Deutsch)

Transformation der Stromversorgung und Bedeutung von Digitalisierung und Cyber-Sicherheit

Cyber-Sicherheit und Resilienz werden zu immer zentraleren Bestandteilen der Schweizer Stromversorgungssicherheit. Die Transformation der Stromversorgung allgemein und die Dezentralisierung im Besonderen, ziehen eine Digitalisierung als Imperativ nach sich. Nur mit ihr lassen sich die vielen dezentralen Ressourcen überwachen, steuern und effizient in das sowieso bereits komplexe Stromversorgungssystem einbinden. Durch die zunehmende Anwendung digitaler Technologien, wie beispielsweise digitale Monitoring- und Steuerungssysteme, der Einsatz intelligenter Messsysteme (Smart Meter) oder die Nutzung von Flexibilität durch Internet-of-Things (IoT) Technologien, findet eine immer stärker werdende Verschmelzung der Informationstechnologie- (IT) und der operationellen Technologie-Landschaft (OT) statt.

Eine klassische, physische Trennung der beiden Welten IT und OT ist nicht mehr gegeben und es entstehen daher neue, bisher nicht da gewesene Angriffsvektoren. Entsprechend steigt die potentielle Cyber-Bedrohungslage und die damit verbundenen Risiken rasant an. Die existierenden Schutzkonzepte müssen folglich der neuen Ausgangslage und den technologischen Entwicklungen der Digitalisierung angepasst werden. Dies mit dem Ziel, um künftige Krisensituationen, wie beispielsweise dem Auftreten grossflächiger «Blackouts», auch weiterhin möglichst erfolgreich vermeiden und die Stromversorgungssicherheit gewährleisten zu können. Die Transformation und die fortschreitende Digitalisierung des Stromversorgungssystems kann nur mit einer robusten Cyber-Sicherheit und Resilienz erfolgreich bestritten werden.

Sinn und Zweck der vorliegenden Analyse

Damit die Schweiz perspektivisch gerüstet ist für die Digitalisierung im Stromsektor, gilt es ein gesamtheitliches Konzept zur Gewährleistung von Cyber-Sicherheit und Resilienz über alle Akteure des Stromversorgungssektors zu erarbeiten. Zunächst wurde dafür die aktuelle Sachlage bezüglich Cyber-Sicherheit und Resilienz im Schweizer Stromversorgungssektor untersucht. Danach wurde der Blickwinkel erweitert und aktuelle, international derzeit verfolgte Ansätze analysiert. Im Quervergleich wurde dann ein allfälliger Handlungsbedarf für die Schweiz identifiziert. Anhand einer im Rahmen dieses Berichts durchgeführten Studie wurde ebenfalls die praktische Notwendigkeit des ermittelten Handlungsbedarfs überprüft. Schliesslich wurden verschiedene Optionen zur Adressierung der Handlungsfelder vorgeschlagen. So kann über die Zeit die Cyber-Sicherheit und Resilienz innerhalb des Schweizer Stromsektors Schritt für Schritt verbessert, das aktuelle Maturitätsniveau angehoben und die Transformation des Sektors inklusive seiner fortschreitenden Digitalisierung sicher gestaltet werden.

Fragmentierung der regulatorischen Vorgaben im Stromsektor betreffend Cyber-Sicherheit

Die Schweiz verfügt im Stromversorgungssektor bereits über Ansätze und gewisse regulatorische Rahmenbedingungen, die für Cyber-Sicherheit und Resilienz beigezogen werden können. Historisch gesehen haben diese Rahmenbedingungen die Versorgungssicherheit im Allgemeinen im Fokus. Die Analyse zeigt, dass eine starke Fragmentierung bezüglich Cyber-Sicherheit vorherrscht. Bestehende Gesetze müssen für die Zwecke der Cyber-Sicherheit teilweise weit interpretiert und ausgelegt werden. Cyber-Sicherheit ist weder einheitlich noch umfassend oder flächendeckend für alle relevanten Akteure

geregelt. So bestehen beispielsweise vereinzelte Grundlagen und für gewisse Akteure verbindliche Pflichten in bestimmten, teilweise untergeordneten Teilbereichen wie etwa beim Einsatz von Smart Metern, oder für den Betrieb von Nuklearkraftwerken. Als Folge der fragmentierten Gesetzeslandschaft sind derzeit unter anderem auch die Rollen und Verantwortungen betreffend Cyber-Sicherheit und Resilienz innerhalb des Stromsektors noch nicht gänzlich klar geregelt und voneinander abgegrenzt.

Viele bestehende Grundlagen sind zudem heute Richtlinien von freiwilliger Natur. Hier sind insbesondere der «IKT Minimalstandard» des Bundesamts für Wirtschaftliche Landesversorgung (BWL) und das «Handbuch Grundschutz für Operational Technology» des Branchenverbands Schweizer Elektrizitätswirtschaft (VSE) erwähnenswert. Eine transparente Gesamtübersicht über alle bestehenden Regelungen und Akteure, sowie eine Analyse deren Zusammenwirkens und der Effektivität fehlt bisher. Der Bund hat diesen Missstand erkannt und gibt mittels der Nationalen Strategie zum Schutz vor Cyber-Risiken (NCS), welche bereits seit 2012 besteht und für die Periode 2018-2022 ausgeweitet wurde, eine korrigierende Richtung vor.

Die Schweiz im internationalen Vergleich

Mittels Quervergleich mit anderen Ländern betreffend regulatorische Situation für Cyber-Sicherheit und Resilienz im jeweils lokalen Stromsektor wurde erkannt, dass die grundsätzliche Stossrichtung der Schweizer NCS 2018-2022 auch in anderen Ländern auffindbar ist.

Insbesondere die Entwicklungen innerhalb der EU sind relevant, da eine sehr starke technische und organisatorische Vernetzung der Stromsysteme der Schweiz und der EU-Mitgliedstaaten besteht, vor allem mit den unmittelbaren Nachbarländern. Entsprechend gross sind die wechselseitigen Abhängigkeiten voneinander. In Europa ist vor allem die Richtlinie für die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) massgebend, welche 2016 in Kraft trat. Die vorliegende Analyse zeigt, dass die in der NCS 2018-2022 festgehaltenen Stossrichtungen des Bundes grösstenteils mit den Massnahmen dieser ersten NIS-Richtlinie der EU kompatibel sind. Dies ist grundsätzlich als positiv zu bewerten.

Jedoch erscheint der aktuelle Vorsprung der EU Staaten im Bereich der Cyber Sicherheit und Resilienz derzeit beachtlich. Viele der für die Schweiz aktuell diskutierten Massnahmen sind aufgrund der NIS-Richtlinie andernorts in der EU bereits in der Praxis umgesetzt, operativ und längst etabliert. Dieser Vorsprung der umliegenden europäischen Länder wird sich zumindest kurzfristig noch wesentlich vergrössern. So wird in der Europäischen Union die NIS-Richtlinie aktuell bereits mit Hochdruck überarbeitet und nochmals weiterentwickelt. Eine zeitnahe Inkraftsetzung ist naheliegend und wird die Cyber-Fähigkeiten der europäischen Akteure auch im Strombereich nochmals erhöhen. Spezifisch für den Stromversorgungssektor wird ebenfalls flankierend zusätzlich noch ein Netzwerk-Kodize «Cyber-Security» derzeit erarbeitet, welcher technische Anforderungen an Netzbetreiber und -anschlussnehmer konkretisieren wird. Es ist zu erwarten, dass auch dieser Netzwerk Kodize bald in Kraft treten wird.

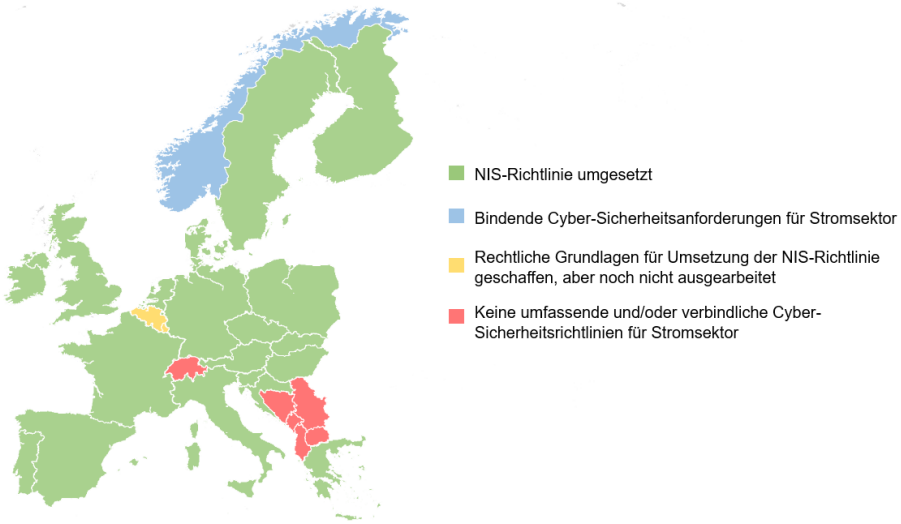


Abbildung MS 1: Europäischer Vergleich betreffend bindenden Sicherheitsanforderungen und Meldepflichten[1]

Cyber Maturität des Schweizer Stromsektors und Ergebnisse der national E-Survey «Cyber»

Zugunsten der aktuellen Lage in der Schweiz liesse sich für den Stromversorgungssektor annehmen, dass aufgrund des geltenden Subsidiaritätsprinzips die Unternehmen der Elektrizitätswirtschaft bisher selbständig und in Eigenverantwortung um Massnahmen zur Gewährleistung der Cyber-Sicherheit und Resilienz besorgt waren. Immerhin ist die Gewährleistung der Versorgungssicherheit ein zentrales Anliegen der Branche und deren Sensibilität diesbezüglich offensichtlich hoch.

Damit allenfalls die richtigen, künftigen Massnahmen für die Schweiz abgeleitet werden können, wurde daher erstmalig die aktuelle Lage betreffend Cyber-Maturität der relevanten Akteure innerhalb der Schweizer Stromversorgung erhoben. Dies erfolgte anhand des seit 2018 durch das Bundesamt für Wirtschaftliche Landesversorgung (BWL) und den Branchenverband Schweizer Elektrizitätswirtschaft (VSE) etablierten «IKT Minimalstandards» und wurde über eine elektronische Umfrage (E-Survey) abgefragt.

Insgesamt wurden etwa 750 Unternehmen um Mithilfe gebeten. Davon beteiligten sich 124 Unternehmen, welche über die verschiedenen Bereiche der Wertschöpfungskette innerhalb des Schweizer Stromsektors tätig sind (vertikal integrierte Unternehmen). Die Mehrheit der in der Umfrage vertretenen Rollen am Markt waren 113 Netzbetreiber gefolgt von 79 Messstellenbetreibern und 54 Produzenten (eine Unternehmung kann zeitgleich mehrere Rollen am Markt wahrnehmen).

Die Auswertungen der Ergebnisse für die Bereiche IT- und OT-Sicherheit zeigen insgesamt beide einen durchschnittlichen Maturitätswert innerhalb des Sektors von knapp unter «1» bei einer Bewertungsskala von «0» bis «4». Diese Werte sind im Schnitt ernüchternd, insbesondere da bei der Verabschiedung der Branchenrichtlinie zum IKT Minimalstandard eine eigens angestrebte Maturität der Branche um den Wert «2.6» kommuniziert wurde.

[1] Eigene Darstellung basierend auf Angaben in Bird & Bird (2020), Developments on NIS Directive in EU Member States.

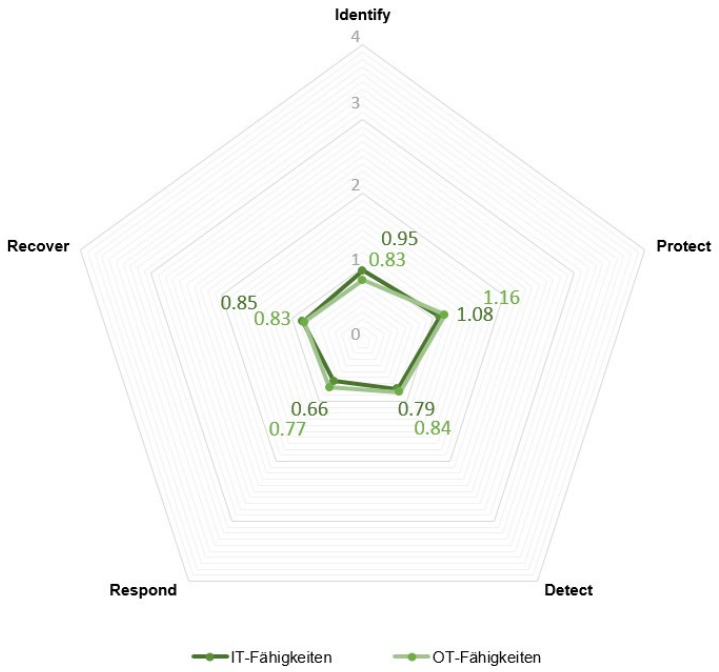


Abbildung MS 2: Durchschn. IKT Maturitätsstand des Schweizer Stromsektors – «E-Survey» Resultate 2020

Vorschläge zur Adressierung der identifizierten Handlungsfelder

Als Resultat der gemachten Analysen und der nationalen E-Survey lässt sich grundlegender Handlungsbedarf für die Schweiz ableiten. Es gilt zunächst, möglichst eine weitere Fragmentierung von Vorgaben in den Bereichen rund um Cyber-Sicherheit und Resilienz innerhalb des Stromsektors zu vermeiden.

Der in dieser Arbeit abgeleitete Handlungsbedarf setzt primär auf den vom Bund definierten Massnahmen der NCS 2018-2022 auf, sowie auf Empfehlungen der 2016 durch das Bundesamt für Energie (BFE) bereits durchgeführten Schutz- und Sicherheitsanalyse im Rahmen der Entwicklung von Smart Grids. Diese wurden als Teil dieser Arbeit sektorspezifisch präzisiert, gezielt erweitert und in ein Gesamtkonzept integriert.

Der für den Schweizer Stromsektor in dieser Arbeit identifizierte Handlungsbedarf gliedert sich primär in vier Handlungsfelder, bei welchen der Schweizer Stromsektor aktuell Weiterentwicklungsbedarf hat. Es wurden verschiedene Optionen zur Adressierung des jeweiligen Handlungsbedarfs erarbeitet und basierend auf einer Analyse der Vor- und Nachteile auch im Rahmen dieses Berichts vorgeschlagen. Es ergab sich zusammenfassend das folgende Bild:

1. Die Schaffung einheitlicher, gesetzlicher Rahmenbedingungen in Bezug auf Cyber-Sicherheit und Resilienz. Dazu gehört unter anderem:
    - Die rechtliche Klärung der Rollen und Verantwortlichkeiten von Wirtschaft und Verwaltungseinheiten bezüglich Cyber-Sicherheit für den Stromversorgungssektor,
    - Die Identifizierung der zu regulierenden Unternehmen innerhalb des Sektors, wofür drei verschiedene Herangehensweisen vorgestellt wurden und die selektive Option zur Ausgestaltung eines verpflichtenden Cyber-Grundschutzes, sowie der Definition weitergehender Anforderungen für bestimmte Marktteilnehmer, empfohlen wurde,
    - Kontinuierliche Sicherstellung der Weiterentwicklung von Cyber-Anforderungen und Rahmenbedingungen in Bezug auf die fortschreitende Digitalisierung und Innovation.

2. Die Sicherstellung einer regelmässigen Überprüfung betreffend die Einhaltung der regulatorischen Anforderungen. Dazu gehört unter anderem:
    - Die Etablierung einer Prüfbehörde, welche in der Lage ist, die Umsetzung von technischen Anforderungen zur Cyber-Sicherheit in der Stromwirtschaft sicherzustellen. Im Bericht wurden drei Optionen zur Ernennung der Prüfbehörde untersucht: das Bundesamt für Energie (BFE), die Eidgenössische Elektrizitätskommission (ElCom) und das Eidgenössisches Institut für Metrologie (METAS),
    - Die Etablierung eines zentralen Registers, welches beispielsweise die jeweiligen Ansprechpartner aller regulierten Unternehmen für die vollziehenden Behörden bereitstellt,
    - Die Einführung von Prüfungsprozessen inkl. deren Ausgestaltung betreffend des zu erbringenden Nachweises zur Einhaltung der regulatorischen Anforderungen. Hierfür wurden verschiedene mögliche Prüfmechanismen präsentiert, wie beispielsweise die Zertifizierungen nach internationalen Standards,
    - Die Ausgestaltung von Selbstbeurteilungsmechanismen durch Marktteilnehmer und die Einführung der Möglichkeit von Stichprobenkontrollen durch die Prüfbehörde,
    - Das Schaffen regulatorischer Rahmenbedingungen und Mechanismen für Sanktionierungen bei allfälliger Nichteinhaltung geltender Gesetze und für gezielte Incentivierungen.

3. Die Einführung eines institutionalisierten Meldewesens betreffend laufender Cyber-Vorfälle innerhalb des Stromsektors Schweiz.
    - Gemäss den Vorgaben des Bundesrats wird das Thema Meldewesen im Stromsektor bereits in einer dedizierten Arbeitsgruppe beim BFE bearbeitet, womit die Etablierung, Ausgestaltung und zeitnahe Umsetzung einer Meldepflicht von Cyber-Vorfällen für die Unternehmen im Stromversorgungssektor Schweiz geklärt werden soll,
    - Das Schaffen regulatorischer Rahmenbedingungen und Mechanismen für Sanktionierungen bei allfälliger Nichteinhaltung von Meldepflichten.

4. Die Institutionalisierung eines regelmässigen Wissensaustausches zu aktuellen Cyber-Gefahren (Threat Intelligence).
    - Die Entwicklung spezifischer Threat Intelligence für den Stromsektor und eines Mechanismus für die schnelle und gezielte Weiterverbreitung innerhalb des Sektors,
    - Der Aufbau gewisser Threat Intelligence Fähigkeiten beim BFE für die Weiterentwicklung von Cyber-Anforderungen unter Berücksichtigung laufender digitaler Innovationen und der dynamischen Cyber-Bedrohungslandschaft.

Entlang dieser vier Handlungsfelder wurde ein übergreifendes Konzept zur künftigen Umsetzung von Cyber-Sicherheit und Resilienz im Schweizer Stromsektor erarbeitet, welches mögliche Handlungsoptionen zur Stärkung des Sektors im Cyber-Bereich transparent aufzeigt, konkrete Handlungsempfehlungen abgibt und ein Zusammenspiel der Massahmen orchestriert.

Schliesslich wurde ein grober Umsetzungsplan skizziert, wie die einzelnen Massnahmen künftig umgesetzt werden könnten. Da die Vorschläge sehr weitreichend sind, wurden die Schritte auch in «zwingend» und «optional» aufgeteilt. Es ist hierbei ebenfalls anzumerken, dass die Mehrheit der Massnahmen gleichzeitig von zentraler Bedeutung ist, um der NCS 2018-2022 sowie den Empfehlungen der bundesrätlichen Expertenkommission zur Zukunft von Datenschutz und Datensicherheit in der Schweiz innerhalb des Stromsektors zu entsprechen.

Executive Summary (Français)

Transformation de l'approvisionnement électrique et importance de la numérisation et de la cybersécurité

La cybersécurité et la résilience deviennent des composantes de plus en plus essentielles de la sécurité de l'approvisionnement électrique en Suisse. La transformation de l'approvisionnement électrique en général et la décentralisation en particulier font de la numérisation un impératif. La numérisation est le seul moyen de surveiller, contrôler et intégrer efficacement les nombreuses ressources décentralisées dans le système d'approvisionnement déjà complexe. En raison de l'utilisation croissante des technologies numériques telles que les systèmes de surveillance et de contrôle numériques, du recours à des systèmes de mesure intelligents (compteurs intelligents) ou de l'exploitation de la flexibilité offerte par les technologies de l'Internet des objets (IoT), on observe une fusion graduelle des technologies de l'information (IT) et du paysage technologique opérationnel (OT).

Etant donné que la séparation physique classique des deux mondes IT et OT n'existe plus vraiment, de nouveaux vecteurs d'attaque jusqu'alors inconnus apparaissent. En conséquence, les cybermenaces potentielles et les risques associés augmentent rapidement. Les concepts de protection existants doivent donc être adaptés au nouveau contexte et aux évolutions technologiques apportées par la numérisation. L'objectif est de continuer à éviter autant que possible de futures situations de crise, telles que la survenue de «pannes» à grande échelle, afin de pouvoir garantir la sécurité de l'approvisionnement en électricité. Une cybersécurité robuste et une bonne résilience sont indispensables pour garantir le succès de la transformation et de la numérisation du système d'approvisionnement électrique.

Signification et objectif de la présente analyse

Pour que la Suisse soit bien préparée à la numérisation dans le secteur de l'électricité, il est nécessaire de développer un concept holistique garantissant la cybersécurité et la résilience de tous les acteurs du secteur de l'approvisionnement électrique. A cette fin, nous avons commencé par analyser la situation actuelle en matière de cybersécurité et de résilience dans le secteur suisse de l'approvisionnement électrique. La perspective a ensuite été élargie et les approches actuellement poursuivies au niveau international ont été analysées. La nécessité d'agir pour la Suisse a ensuite été identifiée sur la base d'une étude comparative. La nécessité pratique du besoin d'action identifié a également été examinée sur la base d'une étude réalisée dans le cadre du présent rapport. Enfin, diverses options ont été proposées pour apporter des améliorations dans les différents champs d'action. Les mesures proposées permettront d'améliorer progressivement la cybersécurité et la résilience du secteur suisse de l'électricité, d'atteindre un niveau de maturité supérieur et de sécuriser la transformation du secteur, y compris sa numérisation croissante.

Fragmentation des exigences réglementaires dans le secteur de l'électricité en matière de cybersécurité

Dans le secteur de l'électrique, la Suisse dispose déjà d'approches et de cadres réglementaires qui peuvent être utilisés pour améliorer la cybersécurité et la résilience. D'un point de vue historique, ces conditions-cadres se sont généralement concentrées sur la sécurité d'approvisionnement. L'analyse révèle une importante fragmentation en termes de cybersécurité. Les lois existantes doivent parfois être interprétées au sens large aux fins de la cybersécurité. La cybersécurité n'est réglée ni uniformément ni complètement ni à grande échelle pour tous les acteurs concernés. Il existe par exemple des bases isolées et des obligations contraignantes pour certains acteurs dans certains sous-domaines, parfois

subordonnés, notamment l'utilisation de compteurs intelligents. Les spécifications pour les exploitants de centrales nucléaires sont définies et vérifiées par l'ENSI. En raison du paysage juridique fragmenté, les rôles et les responsabilités en matière de cybersécurité et de résilience dans le secteur de l'électricité ne sont actuellement pas encore réglementés de manière tout à fait claire et délimités les uns par rapport aux autres.

En outre, de nombreux principes existants sont désormais des lignes directrices à caractère volontaire. Citons en particulier la «norme minimale pour les TIC» de l'Office fédéral pour l'approvisionnement économique du pays (OFAE) et le manuel Protection de base pour les «technologies opérationnelles» OT) dans l'approvisionnement en électricité de l'Association faîtière des entreprises électriques suisses (VSE). Une vue d'ensemble transparente de toutes les réglementations et des acteurs existants, ainsi qu'une analyse de leur interaction et de leur efficacité, fait défaut à ce jour. Le Conseil fédéral a reconnu cette lacune et donne une orientation corrective avec la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), qui existe depuis 2012 et a été étendue à la période 2018-2022.

La Suisse en comparaison internationale

Une comparaison avec d'autres pays concernant la situation réglementaire de la cybersécurité et de la résilience dans le secteur électrique local respectif a permis d'établir que l'orientation de base de la SNPC suisse 2018-2022 se retrouve également dans d'autres pays.

Les développements au sein de l'UE sont particulièrement pertinents en raison de la forte imbrication des systèmes électriques de la Suisse et des États membres de l'UE sur le plan technique et organisationnel, en particulier avec les pays voisins. Les interdépendances mutuelles sont donc importantes. En Europe, la directive sur la sécurité des réseaux et des systèmes d'information (NIS directive), entrée en vigueur en 2016, joue un rôle décisif. La présente analyse montre que les orientations stratégiques de la Confédération énoncées dans la SNPC 2018-2022 sont pour la plupart compatibles avec les mesures de cette première directive SRI de l'UE. Ceci peut être considéré comme positif.

Cependant, l'avance des États de l'UE dans le domaine de la cybersécurité et de la résilience semble actuellement considérable. Bon nombre des mesures actuellement discutées en Suisse ont déjà été mises en œuvre ailleurs dans l'UE conformément à la directive SRI, et sont opérationnelles et établies depuis longtemps. Les pays européens voisins vont encore prendre nettement plus d'avance, du moins à court terme. Dans l'Union européenne, la directive SRI est actuellement en cours de révision et va encore être développée à une cadence rapide. Elle devrait entrer en vigueur rapidement et contribuera à améliorer encore les cybercapacités des acteurs européens du secteur de l'électricité. Spécifiquement pour le secteur de l'approvisionnement électrique, un code de réseau «Cyber-Security» est également en cours d'élaboration et précisera les exigences techniques pour les opérateurs de réseau et les abonnés. Il est à prévoir que ce code de réseau entrera également en vigueur prochainement.

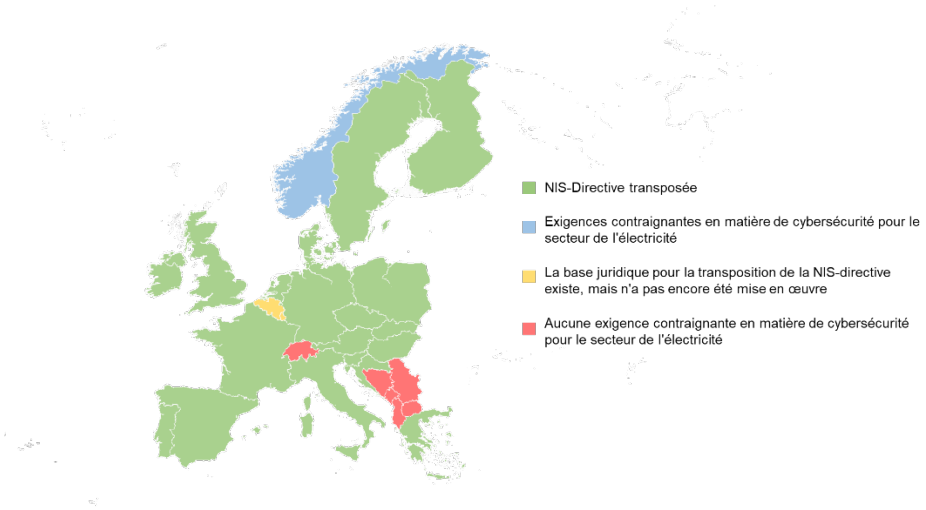


Illustration MS 3: Comparaison européenne concernant les exigences de sécurité contraignantes et les obligations de déclaration[2]

Cybermaturité du secteur suisse de l'électricité et résultats de l'enquête nationale en ligne «Cyber»

Pour expliquer la situation actuelle de la Suisse, pour le secteur de l'électrique, on peut supposer qu'en raison du principe de subsidiarité en vigueur, les entreprises du secteur de l'électricité ont jusqu'à présent mis en œuvre de manière autonome et sous leur propre responsabilité des mesures visant à assurer la cybersécurité et la résilience. Après tout, assurer la sécurité de l'approvisionnement est une préoccupation majeure de la branche et sa sensibilité à cet égard est évidemment élevée.

Afin de pouvoir déterminer les mesures correctes à mettre en œuvre à l'avenir en Suisse, la situation actuelle en matière de cybermaturité des acteurs concernés du secteur de l'approvisionnement électrique en Suisse a été examinée pour la première fois. Cette analyse fondée sur la «norme minimale pour les TIC» établie par l'Office fédéral de l'approvisionnement économique du pays (OFAE) et l'Association faîtière des entreprises électriques suisses (AES) en 2018 a été effectuée au moyen d'une enquête en ligne.

Au total, environ 750 entreprises ont été interrogées. 124 entreprises actives dans les différents domaines de la chaîne de valeur du secteur électrique suisse (entreprises intégrées verticalement) ont participé à l'enquête. 113 opérateurs de réseau représentaient la majorité des rôles sur le marché couverts par l'enquête, suivie de 79 opérateurs de points de comptage et de 54 producteurs (une entreprise peut jouer simultanément plusieurs rôles sur le marché).

Les évaluations des résultats pour les domaines IT et OT montrent toutes deux une valeur de maturité moyenne dans le secteur légèrement inférieure à «1» sur une échelle de notation de «0» à «4». Ces valeurs donnent à réfléchir, d'autant plus que lorsque la directive de branche sur la norme minimale des TIC a été adoptée, une maturité de la branche oscillant autour de «2,6» avait été annoncée.

[2] Présentation propre basée sur les données de Bird & Bird (2020), Developments on NIS Directive in EU Member States.

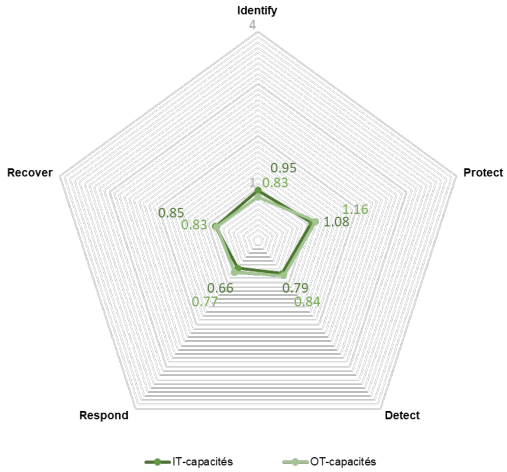


Illustration MS 4: Niveau de maturité TIC moyen du secteur suisse de l'électricité - Résultats de l'enquête en ligne 2020

Propositions d'amélioration dans les champs d'action identifiés

Les résultats des analyses effectuées et de l'enquête nationale en ligne mettent en évidence une nécessité d'agir fondamentale en Suisse. La première chose à faire est d'éviter toute nouvelle fragmentation des exigences dans les domaines de la cybersécurité et de la résilience dans le secteur de l'électricité.

La nécessité d'agir découlant de ce travail repose principalement sur les mesures définies par le Conseil fédéral dans la SNPC 2018-2022, ainsi que sur les recommandations de l'analyse de protection et de sécurité déjà réalisée en 2016 par l'Office fédéral de l'énergie (OFEN) dans le cadre du développement des réseaux intelligents. Dans le cadre de ces travaux, celles-ci ont été précisées spécifiquement pour le secteur, développées de manière ciblée et intégrées dans un concept global.

La nécessité d'agir identifiée pour le secteur suisse de l'électricité dans le cadre de ces travaux se répartit principalement entre quatre champs d'action, dans lesquels la branche doit se développer davantage. Diverses options pour répondre à ces besoins d'action ont été élaborées et sont proposées dans le présent rapport sur la base d'une analyse des avantages et des inconvénients. En résumé, il en ressort l'image suivante:

1. Création d'un cadre juridique uniforme en matière de cybersécurité et de résilience. Cela comprend, entre autres:
    - La clarification juridique des rôles et responsabilités de l'économie et des instances administratives en matière de cybersécurité pour le secteur de l'approvisionnement électrique,
    - L'identification des entreprises à réglementer au sein du secteur
    - L'ancrage et la mise en place d'une cyberprotection de base contraignante, ainsi que la définition d'exigences supplémentaires pour certains acteurs du marché. Trois approches différentes ont été analysées ici et une obligation sélective paraît souhaitable.
    - Assurer en continu le développement des exigences cybernétiques et des conditions-cadres face à la numérisation en cours et à l'innovation.

2. Assurer un contrôle régulier de la conformité aux exigences réglementaires. Cela comprend, entre autres:
    - Mise en place d'une autorité de contrôle capable de garantir l'implémentation des exigences techniques en matière de cybersécurité dans le secteur de l'électricité. Le rapport a examiné trois options pour la nomination de l'autorité de contrôle: l'Office fédéral de l'énergie (OFEN), la Commission fédérale de l'électricité (ElCom) et l'Institut fédéral de métrologie (METAS),
    - La mise en place d'un registre central désignant par exemple les personnes de contact de toutes les entreprises réglementées pour les autorités d'exécution,
    - L'introduction de processus de contrôle, y compris leur conception en ce qui concerne les preuves à fournir concernant la conformité aux exigences réglementaires. Différents mécanismes de contrôle envisageables ont été présentés à cet effet. Il semble avantageux d'externaliser une grande partie des tâches de contrôle à des organes de contrôle externes spécialisés. En outre, l'analyse portait sur la manière dont les preuves devraient être fournies, par exemple via des certifications selon les normes internationales, des audits ou des contrôles aléatoires ou une combinaison de ces moyens,
    - La conception de mécanismes d'auto-évaluation par les acteurs du marché et l'introduction de la possibilité de contrôles aléatoires par l'autorité d'audit,
    - La création d'un cadre réglementaire et de mécanismes de sanctions en cas de non-respect des lois applicables et pour des incitations ciblées.
3. L'introduction d'un système de reporting institutionnalisé des cyberincidents survenus dans le secteur suisse de l'électricité.
    - Sur demande du Conseil fédéral, le sujet du reporting dans le secteur de l'électricité est déjà traité au sein d'un groupe de travail dédié de l'OFEN. Il convient de clarifier l'établissement, la conception et la mise en œuvre en temps voulu d'une obligation de déclaration des cyberincidents pour les entreprises du secteur suisse de l'approvisionnement électrique.
    - La création d'un cadre réglementaire et de mécanismes de sanctions en cas de non-respect des obligations de déclaration.
4. L'institutionnalisation d'un échange régulier de connaissances sur les cybermenaces actuelles (Threat Intelligence).
    - La mise en place d'une veille spécifique sur les menaces pour le secteur de l'électricité et d'un mécanisme de prolifération rapide et ciblée au sein du secteur,
    - La mise en place de capacités de renseignement sur les menaces au sein de l'OFEN en vue de développer les cyberexigences, en tenant compte des innovations numériques en cours et du paysage dynamique des cybermenaces.

Un concept global pour la mise en œuvre future de la cybersécurité et de la résilience dans le secteur suisse de l'électricité a été développé pour ces quatre champs d'action. Ce concept montre de manière transparente les options possibles pour renforcer le secteur dans le cyberespace, fournit des recommandations d'action concrètes et orchestre l'interaction des mesures.

Enfin, un plan de mise en œuvre approximatif a été esquissé sur la manière dont les différentes mesures pourraient être mises en œuvre à l'avenir. Étant donné que les suggestions ont une très grande portée, les mesures ont également été réparties en mesures «contraignantes» et «facultatives». Il convient également de noter que la plupart des mesures sont en même temps d'une importance cruciale pour se conformer à la SNPC 2018-2022 et aux recommandations de la commission d'experts du Conseil fédéral sur l'avenir de la protection des données et de la sécurité des données en Suisse dans le secteur de l'électricité.

Executive Summary (English)

Transformation of power supply and the importance of cybersecurity

Cybersecurity and resilience are becoming increasingly integral to the security of Switzerland's electricity supply. The transformation of power supply in general, and its decentralisation in particular, are making digitalisation indispensable. Through digitalisation the many different decentralised resources can be monitored, managed and efficiently integrated into the already complex power system. Notably, this rising use of digital technologies such as digital monitoring and control systems, of intelligent measuring systems (smart meters) and of the flexibility afforded by Internet of Things (IoT) technologies, increasingly burrs the lines between information technology (IT) and operational technology (OT) landscapes.

Hence, the traditional physical separation between IT and OT is no longer a given, which is leading to the emergence of new attack vectors. The potential cyber-threat situation and the associated risks are intensifying rapidly. Future crises, such as large-scale blackouts, must be avoided and the security of the electricity supply safeguarded. Existing protection concepts thus need to be adapted to the new context and the technological advances in digitalisation. The transformation and advancing digitalisation of the electricity system can only be successfully achieved with robust cybersecurity and resilience capabilities.

Purpose of this report

For Switzerland to be properly equipped to cope with digitalisation in the electricity sector, a holistic concept needs to be developed to guarantee cybersecurity and resilience across all actors in the electricity sector. In a first step the report aimed to analyse the current situation with regard to cybersecurity and resilience in the Swiss electricity sector. The perspective was then widened to understand the latest approaches being pursued internationally. A cross-comparison was conducted to identify any potential need for action for Switzerland. The practical necessity for the identified need for action was also examined based on a survey carried out as part of this report. Finally, various options for addressing the areas of action were proposed. Over time, cybersecurity and resilience within the Swiss electricity sector can be improved incrementally with these recommendations whereby the current maturity levels can be raised, and the transformation of the sector, including its advancing digitalisation, can be made secure.

Fragmented regulatory requirements in the electricity sector with regard to cybersecurity

In the electricity sector in Switzerland, certain regulatory frameworks and general approaches that are applicable for cybersecurity and resilience exist. Yet, the analysis shows that an extensive fragmentation within these requirements prevails. In some cases, existing laws must be interpreted quite broadly to make them relevant for cybersecurity. Overall, cybersecurity is not regulated uniformly, comprehensively or across the board for all relevant actors. For example, there are individual principles and binding obligations applying to certain players in some niche areas, such as the use of smart meters. Rules for nuclear power station operators are set and checked by the Swiss Federal Nuclear Safety Inspectorate (ENSI). As a result of the fragmented legal landscape, the roles and responsibilities within the electricity sector in relation to cybersecurity and resilience are not yet regulated and delineated from one another with complete clarity.

In addition, many of the principles currently in place are voluntary guidelines. The ICT Minimum Standard issued by the Federal Office for National Economic Supply (FONES) and the Basic Protection Manual for Operational Technology ("Handbuch Grundschutz für Operational Technology") of the Association of Swiss Electricity Companies (VSE) are key texts here. However, there is no transparent overview

of all existing regulations and actors. The federal government has recognised this lack and has provided corrective guidance through the National Strategy for the Protection of Switzerland against Cyber Risks (NCS), which has been in existence since 2012 and was expanded for the 2018–2022 period.

International comparison of the situation in Switzerland

A cross-comparison looking at the regulatory situation for cybersecurity and resilience in other countries' local electricity sectors showed that the basic thrust of the Swiss NCS 2018–2022 resembles policies elsewhere.

Developments within the EU are particularly relevant, as Switzerland's electricity systems are very strongly interconnected with those of EU member states, especially its neighbours, from both a technical and organisational standpoint. This means that the mutual interdependencies are also high. In Europe, the main instrument is the Directive on security of network and information systems (NIS Directive), which entered into force in 2016. This analysis shows that the federal government's strategic directions as set out in the NCS 2018–2022 are largely compatible with the measures of this first EU NIS Directive.

However, the EU member states currently appear to have a considerable lead in cybersecurity and resilience. Many of the measures currently being discussed for Switzerland have already been put into practice and are well-established in EU countries as a result of the NIS Directive. Switzerland's neighbours are also likely to pull even further ahead, at least in the short term. This since the European Union is already revising and building on the first version of the NIS Directive at full speed. The updated version should enter into force before long, which will enhance the cyber-capabilities of European players in the electricity sector even further. A cybersecurity network code specifically for the electricity sector is also being developed, which will lay down the technical requirements applicable to network operators and users. This network code is also expected to come into force soon.

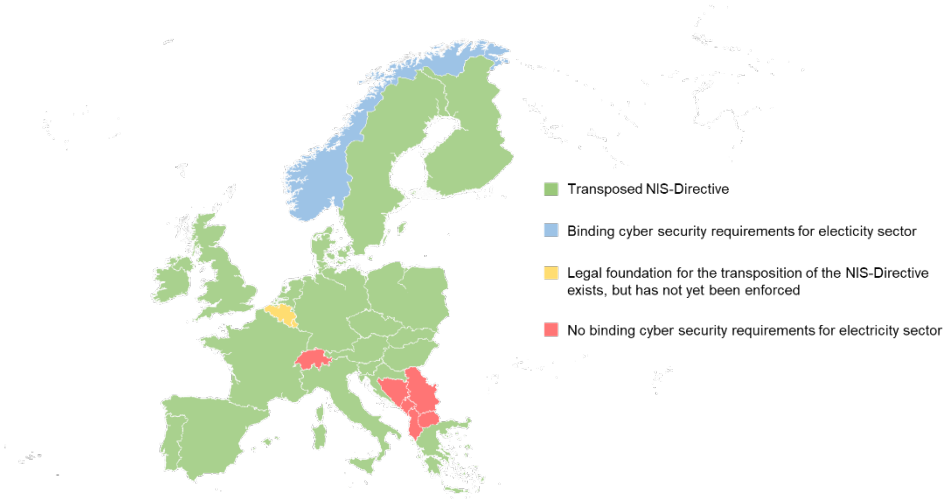


Figure 5: European comparison of binding security requirements and reporting obligations[3]

[3] Own presentation based on information in Bird & Bird (2020), Developments on NIS Directive in EU Member States.

Cyber-maturity of the Swiss electricity sector and results of the national "Cyber" e-survey

In defence of the current situation in Switzerland, it could be argued that, given the principle of subsidiarity, companies in the electricity industry may have already taken charge of their own cybersecurity and resilience independently. After all, ensuring security of supply is a key concern for the industry, and its sensitivity to this issue is high.

The current cyber-maturity of the relevant actors within the Swiss electricity sector was surveyed for the first time to enable a pragmatic approach to developing adequate measures for Switzerland. The questionnaire was based on the ICT Minimum Standards issued by the Federal Office for National Economic Supply (FONES) and the Association of Swiss Electricity Companies (VSE), which have been in place since 2018.

A total of around 750 companies were invited to take part, 124 of them responded. Most of these companies currently operate in different areas along the value chain within the Swiss electricity sector (i.e., they are vertically integrated companies). The most common market role represented in the survey was network operator, with 113 participants. Additionally, 79 metering point operators and 54 producers participated (a company can perform multiple market roles at once).

The evaluation of the results for IT and OT security reveals an average maturity score within the sector of just under 1, on a scale from 0 to 4. These are sobering averages, especially given that when the ICT Minimum Standard was adopted, it was stated that the industry was aiming for a maturity score of around 2.6.

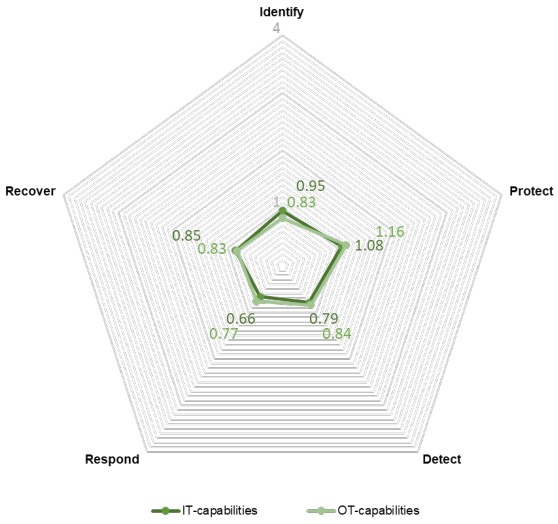


Figure 6: Average ICT maturity of the Swiss electricity sector – survey results 2020

Suggestions for addressing the identified areas of action

A fundamental need for action in Switzerland can be determined based on the findings of the analysis and the national electronic survey. A key concern is to avoid any further fragmentation of cybersecurity and resilience requirements within the electricity sector.

The need for action determined in this report is primarily based on the NCS 2018–2022 measures defined by the federal government, and builds on the recommendations of the protection and security analysis carried out in 2016 by the Swiss Federal Office of Energy (SFOE) in connection with the development of smart grids.

The need for action identified for the Swiss electricity sector in this report is divided into four main areas of action. Various options were developed for addressing each need for action and, based on an analysis of the respective advantages and disadvantages, were proposed for implementation. In short, the concept is as follows:

1. Create a uniform, legal framework for cybersecurity and resilience. This includes:
    - Legally clarify the roles and responsibilities of business and administrative entities with regard to cybersecurity for the electricity sector.
    - Identify the companies to be regulated within the sector.
    - Embed and design mandatory basic cyber protection and define more extensive requirements for certain market participants. Three different approaches were analysed here, whereby a selective approach for the requirements was proposed.
    - Ensure that cyber requirements and operating conditions are refined continuously to reflect advances in digitalisation and innovation.

2. Ensure that compliance with regulatory requirements is reviewed regularly. This includes:
    - Establish an inspection authority ensuring that the technical requirements for cybersecurity in the electricity sector are implemented. The report examined three options for appointing the inspection authority: the Federal Office of Energy (SFOE), the Federal Electricity Commission (ElCom) and the Federal Institute of Metrology (METAS).
    - Establish a central register, which, for example, lists the contact persons at all regulated companies for the enforcement authorities.
    - Introduce inspection processes, which should include procedures for the relevant companies to provide evidence to ensure compliance with the regulatory requirements. Various possible inspection mechanisms were presented, and it appears sensible to outsource a part of the audit work to external, specialist auditors. In addition, an analysis was performed as to how evidence could be provided, as for example via certifications according to international standards, audits, spot checks or a combination of these.
    - Design mechanisms for self-assessment by market participants and introduce the possibility of spot checks by the inspection authority.
    - Create a regulatory framework and mechanisms for sanctions in the event of non-compliance with applicable laws and for targeted incentives.

3. Introduce an institutionalised reporting system for ongoing cyber-incidents within the Swiss electricity sector.
    - In accordance with the instructions of the Federal Council, a dedicated working group at the SFOE is already examining this topic in detail. In general, this work should include clarifying the establishment, design and prompt implementation of an obligation to report cyber-incidents for companies in the Swiss electricity sector.
    - Create a regulatory framework and mechanisms for sanctions in the event of non-compliance with reporting obligations.

4. Put in place regular knowledge-sharing on current cyber-threats (threat intelligence).
    - Develop specific threat intelligence for the electricity sector and a mechanism for rapid and targeted dissemination within the sector.
    - Develop threat intelligence capabilities at the SFOE for the ongoing development of cyber-requirements, considering digital innovations and the dynamic cyber-threat landscape.

An overarching concept for the future implementation of cybersecurity and resilience in the Swiss electricity sector has been outlined along these four areas of action. This transparently shows possible options for strengthening the sector on cyber matters, provides specific recommendations for action and orchestrates the interplay between measures.

Finally, a rough implementation plan was sketched out as to how the individual measures could be implemented. Since the suggestions are far-reaching, the steps were divided into mandatory and optional categories. It also should be noted that the majority of the measures are of central importance to complying with the NCS 2018–2022 and the recommendations of the Federal Council of Experts on the future of data protection and data security in Switzerland within the electricity sector.

Einleitung und Zweck des Berichts

Informations- und Kommunikationstechnologien (IKT) werden zu einem immer integraleren Bestandteil der Wertschöpfungskette der elektrischen Energieversorgung. Unterwerke, Transformatorenstationen und Messstellen werden informationstechnologisch vernetzt und mit der im Stromversorgungsgesetz (StromVG)[4] vorgeschriebenen Einführung von intelligenten Messsystemen (Smart Meter)[5] wird diese Vernetzung zusätzlich regulatorisch verstärkt. Der Prozess der Digitalisierung[6] ermöglicht viele positive Entwicklungen und eröffnet grosse Möglichkeiten für viele wirtschaftliche Aktivitäten, wobei Prozesse vereinfacht oder Ressourceneinsätze reduziert werden können. Beispielhaft ermöglichen Smart Meter dem Netzbetreiber bessere Planungen auf Basis einer verbesserten Datengrundlage und letztlich sogar mehr direkte Eingriffsmöglichkeiten. Die zunehmend bidirektionale Kommunikation zwischen den Systemen bei Unternehmen der Energiewirtschaft und Sensoren im Feld, wie z.B. eben Smart Meter, ermöglicht unter anderem einen effizienteren Systembetrieb ermöglicht. Der Stromsektor wird so zunehmend durch «intelligente» IKT gesteuert und überwacht. So spricht man bereits heute bezüglich des Stromsystems von einem Cyber-Physischem System und digitalen Netzen[7].

Die steigenden Cyber-Risiken im Sektor können dementsprechend bei der Wahrnehmung dieser Chancen nicht ausser Acht gelassen werden. Insbesondere zwei Umstände sind für diese immer wesentlichere Cyber-Bedrohungslage im Stromsektor ausschlaggebend.

Erstens, werden Cyber-Vorfälle vermehrt nicht nur Informationstechnologie (IT)[8] eines Unternehmens betreffen, sondern auch negative Folgen für die Operative Technologie (OT)[9] des betroffenen Unternehmens mit sich bringen.[10] OT-Systeme, wie beispielsweise Supervisory Control and Data Acquisition (SCADA)-Systeme zur Steuerung der Produktionsanlagen, Netzen oder gar Verbrauchern, sind für den Betrieb von diesen kritischen Infrastrukturen sehr bedeutend und wurden historisch gesehen, stets als geschlossene, von der IT-Landschaft physisch abgeschottete Systeme konstruiert. Neue technologische Trends wie 5G Funknetzwerke oder Cloud-Lösungen anstelle physischer Kabel im OT-Bereich lassen diese ehemals strikte, physische Trennung der OT- und IT-Landschaft stetig abschwächen, welches zu einer neuen Cyber-Bedrohungslage im OT-Bereich der Unternehmen führt. Zudem beschäftigte man sich bisher meist mit Cyber-Risiken nur aktiv im IT-Bereich und schütze sich entsprechend. Somit

---

4 Bundesgesetz über die Stromversorgung (Stromversorgungsgesetz, StromVG) vom 23. März 2007 (Stand am 1. Juni 2019).

5 «Smart Meter» tragen zu einem einfachen Endverbraucher- und Mieterwechsel sowie einer stark vereinfachten Stromablesung bei. Die Visualisierung des Verbrauchs fördert Energieeffizienz (Stromeinsparungen) beim Endverbraucher und unterstützt die Verwaltung der dezentralen Produktion, z.B. innerhalb des Eigenverbrauchs. Sie sind wesentliche Bestandteile für den Smart Grid. «Ein Smart Grid ist ein System, das den Austausch elektrischer Energie aus verschiedenartigen Quellen mit Konsumenten verschiedener Verbrauchsprofilen intelligent sicherstellt, d.h. unter Einbezug von Messtechnologien sowie Informations- und Kommunikationstechnologien (IKT).» Bundesamt für Energie (2016a), Risiko- und Schutzbedarfsanalyse für Smart Grids.

6 Für Definition siehe Begriffserklärung am Ende der Einleitung.

7 European Network of Transmission System Operators for Electricity (ENTSO-E; 2019), The Cyber Physical System for the Energy Transition. 2019.

8 Für Definition siehe Begriffserklärung am Ende der Einleitung.

9 Für Definition siehe Begriffserklärung am Ende der Einleitung.

10 Energy Expert Cyber Security Platform (2017), Report - Cyber Security in the Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector.

steigen die Wahrscheinlichkeit, sowie das Ausmass eines Cyber-Vorfalls getrieben durch die Vernetzung der OT-Systeme im Stromsektor erheblich.

Zweitens, erhöht sich mit den fortschreitenden Entwicklungen im Bereich «Internet of Things» (IoT)[11] die Angriffsfläche für mögliche Cyber-Angriffe, da immer mehr Anlagen und Geräte nicht mehr nur Verbraucher innerhalb des Stromsystems darstellen, sondern vielmehr nutzbare Ressourcen für das Stromsystem werden. Die informationstechnische Integration von IoT-Geräten in den Stromsystembetrieb schreitet rasant voran.[12] Die Probabilität für Cyber-Angriffe erhöht sich so dynamisch und es ist ersichtlich, dass einzelne Massnahmen in Bezug auf Betriebsmittel wie intelligenten Messsysteme oder SCADA nicht ausreichen, sondern vielmehr zu einer kontraproduktiven Fragmentierung von Vorgaben und Richtlinien führen, die Fehler und Blind Spots nach sich ziehen können. Vielmehr müssen die Systeme, Datensätze und Netzwerke gesamtheitlich vor Cyber-Risiken geschützt werden.

Aus all den oben genannten Gründen können Cyber-Angriffe im Extremfall immer wahrscheinlicher einen grossflächigen Stromausfall auslösen und somit vermehrt systemrelevante Folgen haben. Hackerangriffe auf Energieinfrastrukturen haben sich zudem insbesondere während der Corona-Pandemie noch zusätzlich vermehrt[13].

Die Cyber-Sicherheit, welche auf den Schutz von IKT vor Cyber-Risiken abzielt, begegnet im Energiesektor insbesondere drei grossen Herausforderungen.[14]

1) Einige Bestandteile des Energiesystems müssen in «Echtzeit» arbeiten, d. h., sie müssen auf Befehle innerhalb weniger Millisekunden reagieren, was die Umsetzung von Cyber-Sicherheitsmassnahmen aufgrund der Zeitbeschränkungen erschwert. Die Abhängigkeit von Verfügbarkeitsanforderungen verstärkt diese Schwierigkeit zusätzlich. Beispielsweise können daher Sicherheitsupdates nur schwer und mit kritischen Verzögerungen implementiert werden.

2) Sogenannte Kaskadeneffekte vervielfachen die Auswirkungen eines Cyber-Vorfalls im Strommarkt massiv, denn Probleme in einem Teil des Netzes können leicht auf andere übergreifen. Diese inhärent starke Vernetzung des Stromnetzes ist aus Sicht der Cyber-Sicherheit aufgrund des «Weakest Link Problems», also, dass die Gesamtsicherheit eines Systems nur so robust ist wie der schwächste Teil davon, besonders leicht angreifbar.

3) Die Kombination aus älteren und modernen Technologien in der Energieinfrastruktur macht das System insgesamt durch das zeitgleiche Bestehen einer Vielzahl an Schnittstellen sehr verwundbar. Typischerweise werden Schutzkonzepte zum Zeitpunkt der Beschaffung eines Systems erstellt, welche natürlicherweise die zu diesem Zeitpunkt bekannten Risiken und Bedrohungen berücksichtigen. Jedoch, wie oben aufgezeigt wurde, können sich diese Bedrohungen und Risiken dynamisch über die Zeit ändern. Die Schutzkonzepte werden aber häufig nicht oder nur verspätet angepasst, da entweder die Interoperabilität der Technologien die nicht zulässt, stark behindert oder die Hersteller der Systeme die benötigten Sicherheitsupdates eingestellt

---

11 Internet of Things (IoT) beschreibt die Vernetzung von Objekten über das Internet, wie z.B. Industriemaschinen, Autos, TV's und Waschmaschinen. Durch diese Vernetzung und die immer grössere Verbreitung von Sensoren in den (Alltags-) Objekten entstehen Milliarden «intelligenter Gegenstände». Eine einheitliche Definition von IoT hat sich unter den unterschiedlichen Akteuren jedoch noch nicht durchgesetzt. Bundesamt für Energie (2018), Digitalisierung im Energiesektor: Dialogpapier zum Transformations-prozess.

12 Energy Expert Cyber Security Platform (2017), Report - Cyber Security in the Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector.

13 Zugehör, D. (2021) Hackerangriffe: Branche sucht Nähe zum BSI.

14 Europäische Kommission (2019), Commission Recommendation on cybersecurity in the energy sector: C(2019) 2400 final.

haben. Diese technologische Fragmentierung bildet entsprechend eine wesentliche Hürde für die Cyber Sicherheit.

Cyber-Sicherheit und Resilienz wachsen so zu einem zentralen Baustein der Versorgungssicherheit, damit Krisensituationen wie insbesondere grossflächige «Blackouts» vermieden werden können. Historisch gesehen wurde aber das Schweizerische Stromversorgungssystem auf eine Art und Weise erschaffen und reguliert, um primär auf Bedrohungsszenarien der physischen Sicherheit einzugehen. Die Zuverlässigkeit bzw. Sicherheit der Stromversorgung wurde priorisiert und die bestehenden Massnahmen basieren vor allem auf dem Prinzip der Redundanz und der entsprechenden Umsetzung von Ausweichmechanismen zollen aber dem Cyber-Physischen Aspekten wenig Tribut. So wurden beispielsweise im Bereich der Kernenergie gewisse sicherheitsrelevante Regelungen bereits eingeführt, bspw. um ein Kernkraftwerk so zu entwickeln und zu bauen, damit die Umwelt vor unbeabsichtigter Freisetzung oder Diebstahl von Kernmaterial geschützt ist. Solche auf physische Risiken ausgelegte Schutzmechanismen sind aber in Anbetracht der fortreitenden Digitalisierung und den erhöhten Cyber-Risiken zwingend weiterzuentwickeln.

In dem Schweizer Stromsektor bestehen bereits einige Initiativen um die Cyber-Sicherheit zu erhöhen, jedoch fehlt ein umfassendes Konzept, welches die bestehenden Fragmente berücksichtigt und so weiterentwickelt, dass Cyber-Sicherheit und Resilienz gewährleistet werden können. Es ist unumgänglich in den IT-/OT-Bereichen für die Schweizer Stromversorgung weitergehende, verpflichtende Vorgaben für Cyber-Sicherheit und Resilienz zu erlassen, um die Sicherheit des Sektors bestmöglich in einer zunehmend vernetzten Welt zu gewährleisten und eine weitere, kontraproduktive Fragmentierung der Cyber-Sicherheit im Stromsektor, z.B. aufgrund weiterer separater Vorgaben an bestimmte Technologien, zu vermeiden.

Eine Schwierigkeit ist hierbei die Berücksichtigung der Vielfalt der Akteure des Stromsektors.[15] Wie in einem späteren Teil des Berichts noch genauer erläutert wird, ist die Struktur des Sektors äusserst komplex. Die Akteure der Stromwirtschaft reichen von Verteilnetzbetreibern (VNB), Übertragungsnetzbetreiber (ÜNB) über sehr verschiedene Arten von Erzeugern der Elektrizität bis hin zu Mess- oder Flexibilitätsdienstleistern. Diese heterogene Prägung des Sektors erschwert eine einheitliche Herangehensweise betreffend Regulierung von Cyber-Sicherheit und Resilienz, da auch die behördlichen Zuständigkeiten hierfür (noch) nicht vollständig geklärt sind.

Das Ziel dieses Berichts ist die Erarbeitung eines gesamtheitlichen Cyber-Sicherheit und Resilienz Konzepts für den Schweizer Stromsektor, um den Sektor besser vor steigenden Cyber-Risiken zu schützen und die Maturität aller Akteure in der Stromversorgung bzgl. Cyber-Sicherheit zu erhöhen. Dies insbesondere vor dem Hintergrund, dass die Cyber-Bedrohungslage zunehmend steigt und langfristig die Anforderungen an die Cyber-Sicherheit von Unternehmen der Elektrizitätswirtschaft folglich zunehmen.

Die Struktur des Berichtes ist entlang der folgenden Kapitel aufgebaut:

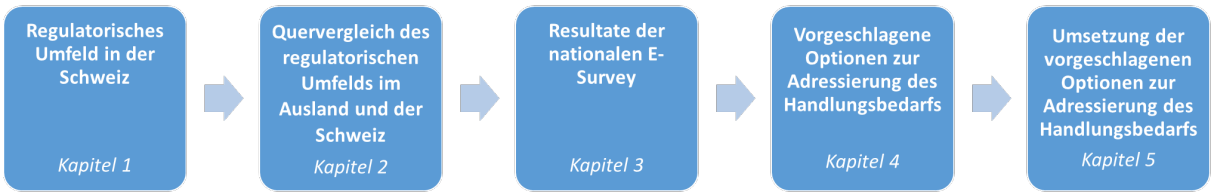


Abbildung 1: Vorgehensweise zur Erarbeitung eines gesamtheitlichen Cyber-Sicherheit und Resilienz Konzept für den Schweizer Strommarkt

[15] Bundesamt für Energie (2017), Bericht - Zuständigkeiten im Bereich der Stromversorgungssicherheit zu Handen der UREK-N.

In Kapitel 1 wird ein Überblick über das aktuelle regulatorische Umfeld betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor gegeben. Ziel dieses Kapitels ist es, ein gemeinsames Grundverständnis bezüglich bereits implementierter, sowie bereits vorgesehener, regulatorischer Massnahmen zu schaffen. Das Kapitel ist in zwei Unterkapitel aufgeteilt. Zu Beginn werden zwei sektorübergreifende, nationale Strategien erläutert, welche grundsätzliche Stossrichtungen des Bundes zum Schutz der Schweiz vor Cyber-Risiken und laufende bzw. künftige vorgesehene Massnahmen angeben. Erst danach wird vertieft auf das bestehende regulatorische Umfeld im Stromsektor eingegangen.

Kapitel 2 führt einen Quervergleich des regulatorischen Umfelds zwischen dem Ausland und der Schweiz durch, wobei unterschiedliche Regulierungsansätze aufgezeigt werden. Die Absicht dieses Kapitels ist die anschliessende Identifikation der Handlungsfelder für den Schweizer Stromsektor im Einklang mit der nationalen Cyber-Sicherheit Strategie des Bundes, in welcher das angestrebte Konzept betreffend Cyber-Sicherheit und Resilienz anschliessend Lösungsoptionen aufzeigen soll. Der Vergleich zielt also keinesfalls darauf ab, die Anforderungen der USA oder EU in der Schweiz unverändert zu übernehmen und dient lediglich als zusätzliche Richtschnur zur Einordnung der regulatorischen Ansätze.

Kapitel 3 befasst sich mit den Auswertungsresultaten der durch das BFE als Teil dieser Studie im Jahr 2020 durchgeführten «E-Survey» bezüglich aktuelles Maturitätsniveau in Cyber-Sicherheit und Resilienz der Marktteilnehmer des Schweizer Stromsektors. Ziel hierbei ist es festzustellen, ob der in Kapitel 2 durch theoretische Grundlagen identifizierte Handlungsbedarf in der Praxis aktuell für die Schweiz ebenfalls eine praktische Herausforderung darstellt.

In Kapitel 4 werden Optionen zur Adressierung des vorgängig identifizierten Handlungsbedarfs erarbeitet. Diese stellen in ihrer Gesamtheit ein Konzept für die künftige Ausgestaltung von Cyber-Sicherheit und Resilienz im Schweizer Stromsektor dar.

In Kapitel 5 werden die Vorschläge in einem groben Umsetzungsplan, welcher die Schritte und deren etwaige zeitliche Abfolge zur Erreichung des Zielzustands aufzeigt, angegeben. Da der vorgeschlagene Zielzustand daraus ambitiös ist, sind die Schritte in ‘zwingend’ und ‘optional’ unterteilt. Somit wurden grosse Ziele gesetzt, welche Schrittweise über einen längeren Zeitraum zu erreichen sind.

Begriffserklärungen

C-I-A-Triade beschreibt die drei klassischen Cyber-Schutzziele der Vertraulichkeit (**C**onfidentiality), der Integrität (**I**ntegrity) und der Verfügbarkeit (**A**vailability) von Daten, Diensten und Systemen. Vertraulichkeit bezieht sich darauf, dass Informationen nur von den Personen eingesehen oder offengelegt werden dürfen, auch dazu berechtigt sind; Integrität bedeutet, dass es nicht möglich sein darf, Informationen unerkannt bzw. unbemerkt zu ändern; Verfügbarkeit beschreibt die Verhinderung von Systemausfällen.

Cyber-Sicherheit, engl. cyber security: anzustrebender Zustand, bei dem die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert.[16] Die Bereiche der IT- und OT-Sicherheit werden als zwei zentrale Unterkategorien der gesamtheitlichen Cyber-Sicherheit anerkannt.

Digitalisierung ist ein Prozess der durch die Möglichkeiten der modernen IKT getrieben wird. Dabei spielen Daten und Informationen eine herausragende Rolle. Digitalisierung lässt sich grundsätzlich in drei Bereiche unterteilen: 1) physische Messinfrastruktur elektronischer Natur; Beispiel: Sensoren zur Akquisition von digitalen Daten und Informationen. Dieser Bereich wird englisch auch «Digitization» genannt. 2) Dateninfrastruktur; Beispiel: Bearbeiten und Vernetzen von Daten. 3) Applikationen; Anwendungen und Automatisierungen. Cyber-Sicherheit und Cyber-Resilienz sind ein integraler Bestandteil der Digitalisierung und betreffen alle drei Bereiche.[17]

Energie- / Stromsektor: Elektrizität bzw. Strom ist nur einer von vielen Energieträgern. Es ist anzumerken, dass dieser Bericht auf den Stromsektor fokussiert ist. Die Verwendung des Begriffs «Energie» betrifft im Rahmen dieser Arbeit daher nur den Teilsektor der Stromversorgung. Erdgas oder Erdöl als Energieträger und die dazugehörigen Versorgungssysteme sind Teilsektoren des Energiesektors, werden im Weiteren nicht berücksichtigt.

Information Technology (IT) sind Technologien zur Datenverarbeitung, welche nicht direkt mit der Bereitstellung von Elektrizität zu tun haben (z.B. Kundendatenmanagement, Personaldatenmanagement, Büroanwendungen). Unter «IT-Sicherheit» werden alle organisatorischen und technischen Massnahmen zum Schutz der Verfügbarkeit, Unversehrtheit (Integrität) und Vertraulichkeit von Informationen verstanden.[18]

Operational Technology (OT) sind Technologien, welche über die Verwendung von IT direkt für die Bereitstellung oder Lieferung von Elektrizität notwendig sind (z.B. SCADA, Fernzugriff auf Installationen in Unterwerken, Rundsteuerung, Energiedatenmanagement, Smart Meter. Unter «OT-Sicherheit» werden alle organisatorischen und technischen Massnahmen zum Schutz der Verfügbarkeit, Unversehrtheit (Integrität) und Vertraulichkeit von Informationen zur Überwachung und Steuerung der Anlagen zur Elektrizitätsverteilung (und -produktion) sowie der Schutz von Personen und Anlagen verstanden.[19]

Resilienz ist die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und das ordnungsgemässe Funktionieren zu erhalten oder dieses möglichst rasch und vollständig wiederzuerlangen.[20]

---

16 Schweizer Cyberrisikenverordnung (CyRV), Art.3 a.

17 Bundesamt für Energie (2018), Digitalisierung im Energiesektor: Dialogpapier zum Transformationsprozess.

18 Eidgenössische Elektrizitätskommission (2019), Bericht - Cyber-Sicherheit 2019. S. 13.

19 Eidgenössische Elektrizitätskommission (2019), Bericht - Cyber-Sicherheit 2019. S. 7.

20 CyRV, Art.3 d.

1 Regulatorisches Umfeld in der Schweiz

Wie in der Einleitung gezeigt wurde, steigt die Cyber-Bedrohungslage im Stromsektor zunehmend, womit die Cyber-Sicherheit ein zentrales Thema zur Sicherstellung der Stromversorgung wird.

Das Ziel dieses ersten Kapitels ist es, einen Überblick über die aktuelle Ausgangslage betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor zu erarbeiten. Diese Analyse ist für die Ableitung von allfällig weiteren nötigen Massnahmen und Instrumenten zur Stärkung der Cyber-Sicherheit und Resilienz sowie zur Umsetzung des angestrebten Gesamtkonzeptes wichtig.

Im ersten Teil dieses Kapitels werden allgemeine, sektorübergreifende Massnahmen betreffend Cyber-Sicherheit und Cyber-Resilienz in der Schweiz vorgestellt.

Die nationale Strategie zum Schutz Kritischer Infrastrukturen (SKI), sowie die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022 zeigen die generelle strategische Richtung zur Bekämpfung von Cyber-Risiken in der Schweiz auf. Das Ziel der SKI ist es die Resilienz, also die Widerstands-, Anpassungs- und Regenerationsfähigkeit, der Schweiz im Hinblick auf Kritische Infrastrukturen (KI)[21] weiter zu verbessern. Das Ziel der NCS ist die nationale Stärkung der Cyber-Sicherheit, damit bei der Nutzung der Chancen der Digitalisierung die Schweiz zum einen angemessen vor Cyber Risiken geschützt und zum anderen diesen gegenüber resilient ist.

Es gib einige Schnittstellen zwischen den Strategien, da beide teilweise den Schutz von KI regeln. Zusätzliche Komplexität ergibt sich auch dadurch, dass unterschiedliche staatliche Akteure für die koordinierte Umsetzung der Strategien zuständig sind. Das Bundesamt für Bevölkerungsschutz (BABS) ist für die Koordination zur Umsetzung der SKI zuständig und das Nationalen Zentrum für Cyber-Sicherheit (NCSC) zusammen mit den jeweiligen Fachämtern analog für die NCS.

Das Zusammenspiel dieser Schnittstellen wird in der untenstehenden Abbildung dargestellt, sowie in der nachfolgenden Analyse genauer erläutert.

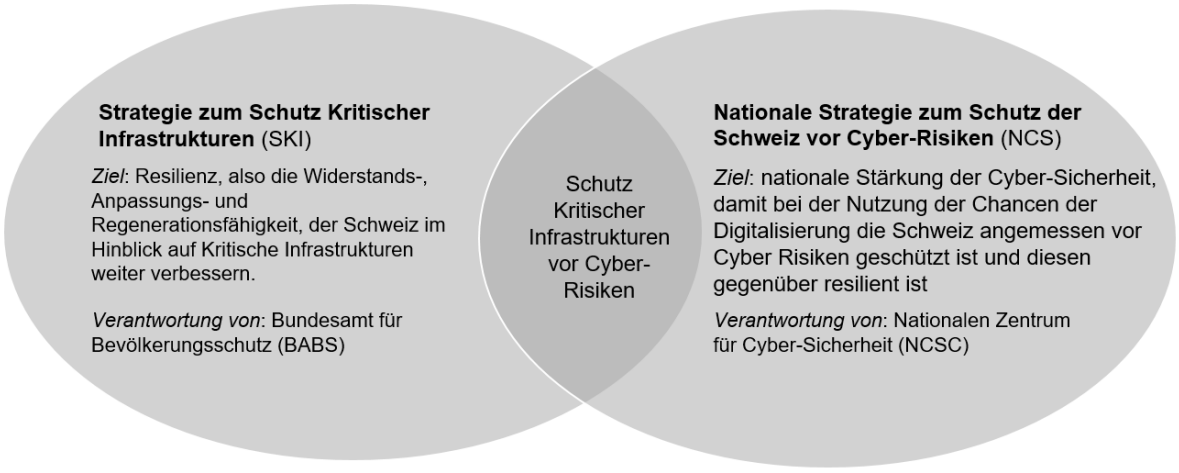


Abbildung 2: Schnittstelle der Strategie zum Schutz Kritischer Infrastrukturen und Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

[21] Nicht zu verwechseln mit Künstlicher Intelligenz, welche ebenfalls gemeinhin mit «KI» abgekürzt wird.

Im zweiten Teil dieses Kapitels wird auf die bestehenden Anforderungen spezifisch für den Stromsektor eingegangen, welche relevant sind in Bezug auf Cyber-Sicherheit.

1.1 Strategische Vorgaben des Bundes

In diesem Teil des ersten Kapitels werden die Massnahmen auf nationaler Ebene zum Schutz der Schweiz vor Cyber-Risiken erläutert. Diese Vorgaben zeigen eine Richtung, die bei der Ableitung des Konzepts für Cyber-Sicherheit und Resilienz für den Schweizer Strommarkt zu berücksichtigen sein werden.

1.1.1 Nationale Strategie zum Schutz vor Cyber-Risiken 2018-2022 (NCS)

Mit der neu erarbeiteten Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-2022 (NCS) verfolgt der Bundesrat das Ziel, Cyber-Risiken aktiv entgegenzutreten und die nötigen Massnahmen zu ergreifen, um die Sicherheit des Landes vor den Bedrohungen im Cyber-Raum[22] zu wahren. Mit dem in Kraft treten der Cyberverordnung am 1. Juli 2020 übernimmt das Nationalen Zentrum für Cyber-Sicherheit (NCSC) die Aufgabe für die koordinierte Umsetzung der NCS 2018-2022[23].

Die Strategie soll dazu beitragen, dass die Schweiz bei der Nutzung der Chancen der Digitalisierung angemessen vor Cyber-Risiken geschützt und ihnen gegenüber resilient ist. Aus dieser Vision abgeleitet, identifiziert die NCS sieben strategische Ziele, welche mit 29 Massnahmen in insgesamt zehn Handlungsfeldern erreicht werden sollen.[24] Die Handlungsfelder und Massnahmen sind in Anhang 2 angefügt. Der Fokus liegt hierbei besonders auf dem Schutz KI, zu denen die Versorgungsinfrastrukturen des Stromsektors gehören.[25]

Grundsätzlich geht die NCS von einem risikobasierten Ansatz aus, welcher zum Ziel hat, die Resilienz der Schweiz hinsichtlich Cyber-Risiken zu verbessern. Dies impliziert die Annahme, dass kein vollständiger Schutz vor Cyber-Risiken möglich ist, die Risiken aber soweit behandelt werden können, dass das verbleibende Risiko tragbar ist.

---

[22] Der Cyber-Raum umfasst die Gesamtheit der Informations- und Kommunikationstechnik (IKT, d.h. Hard- und Software), die untereinander Daten austauschen, diese erfassen, speichern, verarbeiten oder in (physische) Aktionen umwandeln, sowie die dadurch ermöglichten Interaktionen zwischen Personen, Organisationen und Staaten.

[23] CyRV Art 12 f. Das NCSC koordiniert die Umsetzung der NCS, führt ein strategisches Controlling durch und bereitet die Sitzungen der KGCy und des StA NCS vor.

[24] Die Handlungsfelder und Massnahmen sind in Anhang 2 angefügt.

[25] Erdgasversorgung, Erdölversorgung und Fern- und Prozesswärme als kritische Teilsektoren des Energiesektors sind auch von der NCS betroffen (vgl. Kapitel 1.1.2 betreffend SKI). Diese sind aber ausserhalb des Fokus dieses Berichts, weshalb nicht weiter spezifisch auf die Auswirkung der NCS auf den Teilsektoren eingegangen wird.

Abbildung 3 fasst die Inhalte der NCS zusammen:

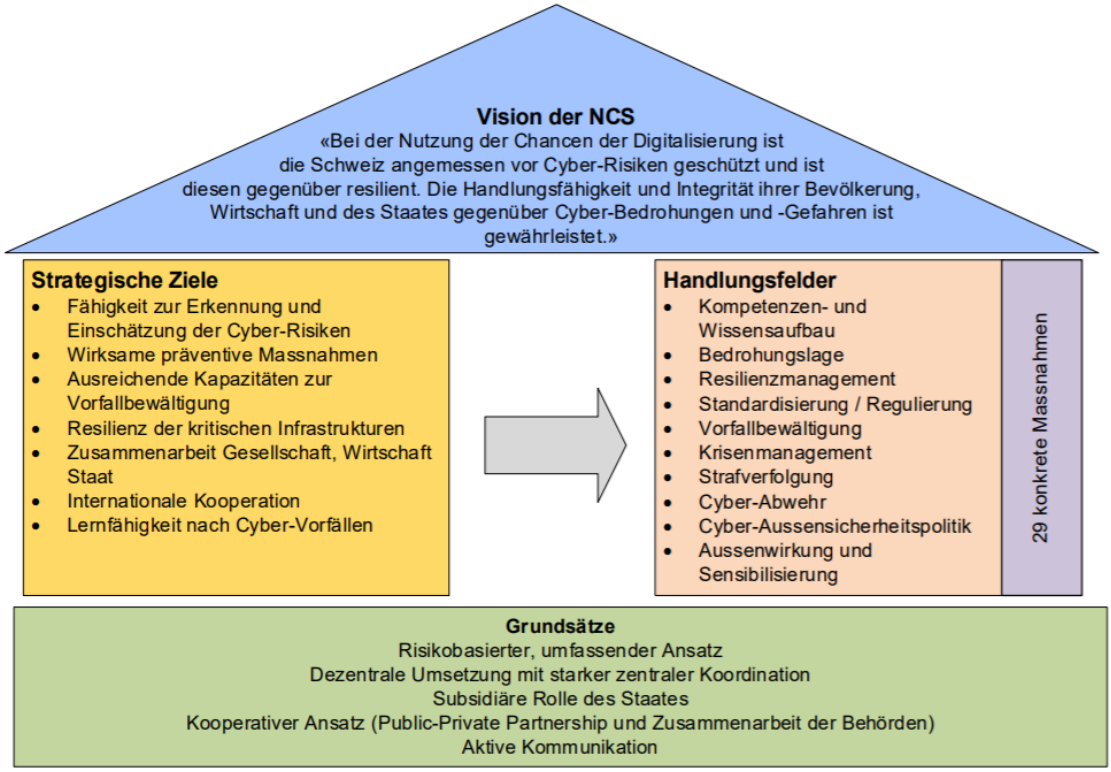


Abbildung 3: Inhalte der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken[26]

Das NCSC, welches wie erwähnt für die koordinierte Umsetzung der NCS 2018-2022 zuständig ist, ist die zentrale Anlaufstelle des Bundes für alle Cyber-Thematiken. Es ist eng mit Sektor-Experten der Fachämter innerhalb des internen Expertenpool (vgl. Abbildung 4) verknüpft. Der NCSC-zugehörige zentrale Expertenpool steht den Fachämtern bei der Entwicklung und Umsetzung von Massnahmen zur Cyber-Sicherheit, sowie technischen Fragen zur Verfügung. Der Expertenpool soll insbesondere dazu beitragen, dass das Sektor-spezifische Wissen und die rechtlichen Kompetenzen bei Bedarf und projektbezogen mit Cyber-Fachwissen ergänzt werden.

Die Melde- und Analysestelle Informationssicherung (MELANI) mit dem nationalen Computer Emergency Response Team (GovCERT)[27] wurde als technische Fachstelle in das NCSC integriert und weiter ausgebaut (vgl. Abbildung 4). Der Zweck von MELANI ist sowohl die Früherkennung von Gefahren und deren Bewältigung, sowie die Unterstützung der Betreiber von KI in der Krise.

---

[26] Abbildung aus NCS 2018-2022 Umsetzungsplan, S. 4.

[27] Die Kernaufgabe eines Computer Emergency Response Team (CERT) ist die Prävention, Detektion und Bewältigung von IT- und Netzwerk-Vorfällen, welche seine Kunden betreffen. Das CERT-Team besteht aus IT-Sicherheitsspezialisten und arbeitet eng und auf hohem Vertrauensniveau mit seinen Kunden zusammen. Aufgrund der internationalen Dimension benötigt ein CERT-Team neben einem sehr guten nationalen auch ein weltweites Netzwerk von Vertrauensbeziehungen auf operativer IT-Security-Ebene. Im Gegensatz zu einem Security Operations Center (SOC), sind CERTs eher eine Notfallorganisation, welche sich um detaillierte Analysen und sich mit der Behebung von Sicherheitsvorfällen beschäftigt. SOC und CERT ergänzen sich und bilden somit eine leistungsfähige Einheit für die Cyber-Sicherheit. CERT und CSIRT wurden in dem Bericht synonym verwendet.

Der Bereich des Eigenschutzes bezieht sich auf die Kompetenz des NCSC, dass es als Fachstelle IKT-Sicherheit (IKT-SEC) des Bundes Vorgaben zur Cyber-Sicherheit innerhalb der Bundesverwaltung erlassen kann. Dies beinhaltet die Überprüfung und Einhaltung der Vorgaben sowie Unterstützung der Leistungserbringer bei der Beseitigung von Schwachstellen (VULN-MGNT). Öffentliche Informationen zu dem Zuständigkeitsbereich der Cyber Diplomatie (Cyber Dipl.), welches dem Eidgenössisches Departement für auswärtige Angelegenheiten (EDA) zugehört, stehen noch aus.

Abbildung 4 verdeutlicht die Struktur des NCSC:

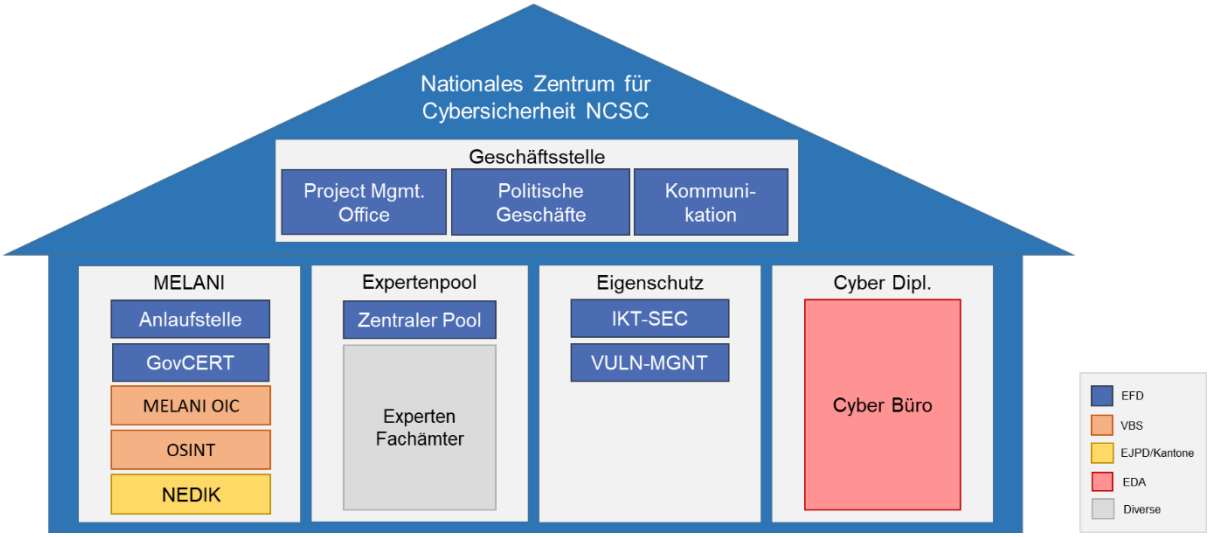


Abbildung 4: Organisation des Nationalen Zentrum für Cyber-Sicherheit [28]

[28] Abbildung von NCSC-Website (2020): https://www.ncsc.admin.ch/ncsc/de/home/ueber-ncsc/das-ncsc.html
Erläuterung Abkürzungen: MELANI Operation Information Center (MELANI OIC), Open Source Intelligence (OSINT), Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK), Eidgenössisches Finanzdepartement (EFD), Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), Eidgenössisches Justiz- und Polizeidepartement (EJPD).

Wie bereits erwähnt ist die NCS entlang von zehn Handlungsfelder und 29 Massnahmen aufgebaut (vgl. Anhang 2). Aufgrund des Schwerpunkts dieses Berichts auf den Stromsektor sind gewisse Aspekte hervorzuheben (vgl. Tabelle 1). Die Selektion der Aspekte ist damit zu begründen, dass das BFE als Fachamt und/oder die ElCom als Regulator und/oder der Stromsektor als Zielgruppe der Massnahme erwähnt werden.

Tabelle 1: Massnahmen der NCS 2018-2022 mit Relevanz für Cyber-Sicherheit und Resilienz Konzept für Schweizer Stromsektor

Handlungsfeld	Massnahme	Beschreibung
Bedrohungslage	**Massnahme 4:** Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage	*Verantwortung:* Nachrichtendienst des Bundes Die gewonnenen Erkenntnisse zur Bedrohungslage sind systematisch aufzuarbeiten, regelmässig zu aktualisieren und über den Lageradar zielgruppengerecht darzustellen.
Resilienz-Management	**Massnahme 5:** Verbesserung der IKT-Resilienz der Kritischen Infrastrukturen	*Verantwortung*: BABS in Zusammenarbeit mit den Fachämtern in regulierten Sektoren Im Fokus steht die Umsetzung von Massnahmen zur Verbesserung der IKT-Resilienz der kritischen Teilsektoren unter Einbezug der relevanten Regulierungsbehörden und Fachämter. Grundlagen dafür sind die vorhandenen Risiko- und Verwundbarkeitsanalysen (vgl. Anhang 3) und die daraus abgeleiteten Massnahmenvorschläge.
Standardisierung / Regulierung	**Massnahme 8**: Evaluierung und Einführung von Minimalstandards	*Verantwortung*: BWL *Beteiligung*: NCSC, BABS, Fachämter (BABS, BAG, BAKOM, BAV, BAZL, BFE) Auf der Basis der durchgeführten Risiko- und Verwundbarkeitsanalysen werden in enger Zusammenarbeit zwischen den Fachbehörden, der Privatwirtschaft und den Verbänden IKT-Minimalstandards evaluiert und eingeführt. Wo vorhanden, werden bestehende Standards verwendet und allenfalls adaptiert. <u>*Relevante Entwicklung seit Veröffentlichung NCS*</u>: - Basierend auf einem Bericht der der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit beschloss der Bundesrat, dass, angesichts der fortschreitenden Digitalisierung, verpflichtende Sicherheitsstandards zu prüfen sind und bis Ende 2022 Lösungsoptionen aufzuzeigen sind.[29] Es wird gefordert, dass Bund und Kantone in enger Zusammenarbeit mit den Fachverbänden auditierbare IKT-Sicherheitsstandards erarbeiten und die Betreiber von KI verpflichten, diese Sicherheitsstandards einzuhalten.

[29] Bundesrat (2018a), Medienmitteilung: Bundesrat nimmt Schlussbericht der Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit» zur Kenntnis.

Handlungsfeld	Massnahme	Beschreibung
Standardisierung / Regulierung	**Massnahme 9**: Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung	*Verantwortung*: NCSC *Beteiligung*: BABS, Fachämter (BAG, BAKOM, BAV, BAZL, BFE), fedpol Zur Verbesserung des Lagebilds zu Cyber-Bedrohungen ist die Einführung einer Meldepflicht für Cyber-Vorfälle zu prüfen und über ihre Einführung zu befinden. Dabei sind zunächst die Fragen zu klären, für wen eine Meldepflicht gelten soll, welche Vorfälle sie betrifft und an wen sie gemeldet werden müssen und ob eine Meldepflicht im Vergleich zu heute das Lagebild substanziell verbessern kann. *Relevante Entwicklungen seit Veröffentlichung NCS:* - In einem Bericht beschreibt der Bundesrat Varianten für Meldepflichten von KI bei schwerwiegenden Sicherheitsvorfällen.[30] Dieser beschreibt die Kernfragen, welche sich in Bezug auf die Einführung von Meldepflichten stellen und zeigt mögliche Modelle zu ihrer Umsetzung auf. - Im Dezember 2020 hat sich der Bundesrat für die Einführung einer Meldepflicht für KI bei Cyber-Angriffen ausgesprochen.[31] Der Bundesrat hat das EFD beauftragt, bis Ende 2021 eine Vernehmlassungsvorlage auszuarbeiten, welche die rechtlichen Grundlagen für diese Meldepflicht schafft. Auf Gesetzesstufe soll dabei eine zentrale Meldestelle bezeichnet und für alle Sektoren einheitlich bestimmt werden. Die konkreten Bestimmungen zur Ausgestaltung der Meldepflicht sollen, angepasst auf die Sektor-spezifischen Gegebenheiten, in entsprechenden Erlassen definiert werden.
Standardisierung / Regulierung	**Massnahme Nr. 11**: Aufbau von Expertise zu Fragen der Standardisierung in Bezug auf Cyber-Sicherheit	*Verantwortung*: NCSC *Beteiligung*: Fachämter (BAG, BAKOM, BAV, BAZL, BFE), Regulatoren (FINMA, ElCom), BABS, BWL, armasuisse W+T, SIF (Verantwortlich für den Beitrag der Schweiz beim Aufbau von Cyber-Kapazitäten in der internationalen Finanzpolitik) Der Bund baut einen Expertenpool zu Fragen der Standardisierung im Bereich Cyber-Sicherheit auf. Der Expertenpool berät die Regulatoren bei der Entwicklung und Umsetzung von themenbezogenen Standards, Regularien oder Leitlinien. Er unterstützt bei Bedarf die Kantone, beobachtet die internationale Entwicklung im Bereich Standardisierung und Regulierung.

[30] Bundesrat (2019), Bericht: Varianten für Meldepflichten von Kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen.

[31] Bundesrat (2020), Medienmitteilung: Bundesrat spricht sich für eine Meldepflicht für kritische Infrastrukturen bei Cyberangriffen aus.

Handlungsfeld	Massnahme	Beschreibung
Krisenmanagement	**Massnahme Nr. 17:** Gemeinsame Übungen zum Krisenmanagement	*Verantwortung*: NCSC *Beteiligung*: Fachämter (BAG, BAV, BAKOM, BFE, BAZL, fedpol), BWL, BABS, BSTB, GS-VBS, SVS In gemeinsamen Übungen von Bund, Kantonen und Vertretern von KI wird das Krisenmanagement in Bezug auf die Cyber-Aspekte getestet. Dabei sind sowohl Cyber-Aspekte in generelle Übungen einzubeziehen, als auch spezifische Übungen zur Bewältigung von Krisen mit Cyber-Ausprägungen durchzuführen. Die Übungen werden ausgewertet und fliessen in die Optimierung der Führungsabläufe und -prozesse ein.

Diese Massnahmen sind zentral für das gesamtheitliche Cyber-Sicherheit und Resilienz Konzept für den Schweizer Strommarkt, da diese die nationale Richtung vorgeben und einigen staatlichen Behörden konkrete Aufgaben auferlegt haben. Wie nachfolgend genauer erläutert wird, sind insbesondere die Entwicklungen nach Veröffentlichung der NCS im Rahmen von Massnahmen 4, 8 und 9 für die Konzeptualisierung des vorgeschlagenen Zielzustands wegweisend.

1.1.2 Nationale Strategie zum Schutz Kritischer Infrastrukturen 2018–2022 (SKI)

Die Umsetzung der nationalen SKI-Strategie erfolgt im Rahmen von bestehenden Strukturen und Zuständigkeiten. Das Bundesamt für Bevölkerungsschutz (BABS) wurde mit der übergeordneten Koordination bei der Umsetzung der Strategie beauftragt. Das von der SKI betroffene Spektrum der KI umfasst neun Sektoren, unterteilt in 27 Teilsektoren (Branchen). Der Sektor Energie umfasst die Teilsektoren Stromversorgung, Erdölversorgung, Erdgasversorgung sowie Fern- und Prozesswärme. Die SKI sieht Massnahmen vor, mit denen die Versorgungssicherheit im Allgemeinen, aber insbesondere im Strombereich erhalten und verbessert werden soll.

Bezüglich der Anwendbarkeit der SKI ist ein periodisch aktualisiertes Verzeichnis (Inventar) erstellt worden, welches Infrastrukturen führt, die für die Schweiz eine strategisch wichtige Bedeutung haben. Die einzelnen Infrastrukturen bzw. Objekte wurden aufgrund ihrer Kritikalität aufgenommen. Kritikalität wird als ein relatives bzw. qualitatives Mass für die Bedeutung verwendet, die ein Ausfall der jeweiligen Infrastruktur für die Bevölkerung und deren Lebensgrundlagen hat.

Das Inventar hilft die Frage zu beantworten, welche Objekte besonders geschützt werden sollen und hilft unter anderem den Bundesstellen und den kantonalen Partnern im Bevölkerungsschutz dazu, bei Katastrophen und Notlagen den Mitteleinsatz zu priorisieren. Zudem dient das SKI-Inventar als Planungsgrundlage für präventive und vorsorgliche Massnahmen oder für Risikoabschätzungen, wie z. B. hinsichtlich Naturgefahren.

Aufgrund der hohen Kritikalität finden sich in diesem Inventar viele Infrastrukturen des Stromversorgungssektors, die eine wesentliche Bedeutung haben für die Versorgung mit Strom, wie z.B. Unterwerke, Produktionsanlagen, etc. Für den Schutz der KI im Stromsektor liegt das Interesse auf den grundlegenden Prozessen und Werken, welche für die sichere, zuverlässige und leistungsfähige Betriebsfähigkeit des schweizerischen Stromsektors essentiell sind. Dies beinhaltet u.a. den sicheren Betrieb der Kraftwerke und Netze, die Systemkoordination, die Netzregelung, die Schwarzstart- und die Inselbetriebsfähigkeit von Erzeugern, die Spannungshaltung etc. Das BABS hat per Ende 2020 ein solches Verzeichnis von Infrastruktur-Objekten erstellt.

Die nationale SKI-Strategie 2018–2022 definiert weiter für alle Akteure übergeordnete Ziele und Handlungsgrundsätze für eine möglichst ununterbrochene Verfügbarkeit von essenziellen Gütern und Dienstleistungen von verschiedenen Sektoren. Zudem bezeichnet sie 17 Massnahmen, mit denen die Resilienz der Schweiz in Bezug auf KI verbessert werden soll. Massnahme 13 ist spezifisch auf den Stromsektor ausgelegt: «Bund und Kantone erstellen vorsorgliche Planungen zur Bewältigung von schwerwiegenden Ausfällen der KI – insbesondere der Stromversorgung – und aktualisieren diese periodisch».

Tabelle 2: Cyber-Aspekte der Strategie zum Schutz Kritischer Infrastrukturen (SKI) 2018–2022

Handlungsfeld	Massnahme	Cyber-Relevanz
Analyse: Verbesserung der Resilienz in den kritischen Sektoren	**Massnahme 1**: Überprüfung und Verbesserung betreffend Resilienz bei KI.	Die KI-Betreiber überprüfen und verbessern ihre Resilienz, beispielsweise gestützt auf den SKI-Leitfaden, in Eigenverantwortung und in Zusammenarbeit mit den zuständigen Fach, Aufsichts- und Regulierungsbehörden. Die zuständigen Aufsichts- und Regulierungsbehörden überprüfen und verbessern die Resilienz in allen kritischen Teilsektoren. Diese Massnahme überschneidet sich direkt mit Massnahme 5 der NCS 2018-2022: «Verbesserung der IKT-Resilienz der kritischen Infrastrukturen».
Analyse: Verbesserung der Resilienz in den kritischen Sektoren	**Massnahme 2:** Prüfung Rechtsgrundlage mit Resilienz-Vorgaben für KI-Betreiber	Das VBS (BABS) prüft in Zusammenarbeit mit den Departementen, ob Sektor-übergreifende Resilienz-Vorgaben notwendig sind. Solche Vorgaben würden auch die Cyber-Resilienz abdecken.
Analyse: Akute Gefährdungen und Bedrohungen frühzeitig erkennen und kommunizieren	**Massnahme 8:** Es ist die Erarbeitung eines Vorschlags für Rechtsgrundlagen zu prüfen, mit der die Betreiber verpflichtet werden, schwerwiegende Sicherheitsvorfälle bzw. Funktionsausfälle den zuständigen Behörden zu melden.	Das VBS (BABS) prüft in Zusammenarbeit u. a. mit dem EFD (ISB) und dem UVEK die Schaffung von Rechtsgrundlagen für eine Pflicht, schwerwiegende Sicherheitsvorfälle und Ausfälle von KI zu melden. Diese Massnahme überschneidet sich mit Massnahme 9 der NCS 2018-2022: «Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung».
Umsetzung und Überprüfung: Massnahmen zum Schutz von KI werden im Rahmen von Übungen auf ihre Praxistauglichkeit getestet	**Massnahme 17:** Im Rahmen von ohnehin geplanten Übungen sollen einzelne SKI-Aspekte gezielt geübt werden.	Die für die Durchführung der Übungen verantwortlichen Stellen bei Bund, Kantonen und KI-Betreibern berücksichtigen SKI-Aspekte bei der Planung und Durchführung von Übungen. Diese Massnahme überschneidet sich mit Massnahme 17 der NCS 2018-2022: «Gemeinsame Übungen zum Krisenmanagement».

Die SKI dient zwar zur Sicherstellung der allgemeinen Versorgungssicherheit, sie anerkennt aber Cyber-Risiken als wesentliches Risiko für KI und verweist explizit auf die NCS. Es ergeben sich Schnittstellen und Synergien zwischen den Massnahmen. Diese Querreferenzen sind in der Tabelle 2 aufgelistet.

Der Bundesrat hat mit Massnahme 1 der nationalen SKI-Strategie die zuständigen Aufsichts- und Regulierungsbehörden beauftragt, in jedem Teilsektor (Stromversorgung, Telekommunikation usw.) zu prüfen, ob Risiken für gravierende Störungen bestehen und nötigenfalls Massnahmen zu deren Reduktion zu erarbeiten. Das BABS koordiniert diese Arbeiten und fokussiert dabei insbesondere auch auf Cyber-Risiken. Damit kann die Massnahme gemeinsam mit der ähnlich lautenden Massnahme 5 (Resilienz-Management) der NCS umgesetzt werden.

Im Stromsektor liegt das Interesse auf den grundlegenden Prozessen und Werken, welche für die sichere, zuverlässige und leistungsfähige Betriebsfähigkeit des schweizerischen Stromsektors essentiell sind. Dies beinhaltet u.a. den sicheren Betrieb der Kraftwerke und Netze, die Systemkoordination, die Netzregelung, die Schwarzstart- und die Inselbetriebsfähigkeit von Erzeugern, die Spannungshaltung etc.

In Ergänzung zu diesen Arbeiten hat der Bundesrat alle Betreiber aufgefordert, ihre Resilienz in Eigenverantwortung zu überprüfen und zu verbessern. Das BABS hat einen Leitfaden und eine Umsetzungshilfe publiziert, die die Betreiber dabei unterstützen. Damit können die Betreiber verschiedene Risiken, die ihre Funktionsfähigkeit beeinträchtigen können, analysieren und Massnahmen definieren, um die Risiken auf ein akzeptables Niveau zu reduzieren. Auch hier sind die Cyber-Risiken Teil eines ganzheitlichen Risiko-Spektrums.

Weitere Massnahmen mit Cyber-Bezug stellen u.a. die Prüfung von Sektor-übergreifenden Resilienz-Vorgaben (Massnahme 2) und die Prüfung einer Meldepflicht bei Ausfällen und Störungen (Massnahme 8) dar. Die untenstehende Tabelle gibt eine Übersicht über die Massnahmen der SKI-Strategie mit Cyber-Bezug.

Im zweiten Teil dieses Kapitels wird auf die bestehenden Anforderungen spezifisch für den Stromsektor eingegangen, welche relevant sind in Bezug auf Cyber-Sicherheit.

1.2 Sektor-spezifische Regulierungsaktivitäten

Innerhalb dieses Kapitels werden aktuelle, Cyber-fokussierte Rahmenbedingungen und Massnahmen, welche spezifisch für den Schweizer Stromsektor von Relevanz sind, aufgeführt.

Zunächst werden die allgemeinen Zuständigkeiten betreffend Stromversorgungssicherheit zwischen dem Bundesamt für Energie (BFE), der Unternehmen der Energiewirtschaft, der Eidgenössischen Elektrizitätskommission (ElCom) und dem Bundesamt für Wirtschaftliche Landesversorgung (BWL) skizziert. Dies zeigt die bisherige bundesweite Organisation für die Versorgungssicherheit bezüglich bestehender Risiken im Stromsektor auf, ohne jedoch spezifisch auf das Cyber-Thema Bezug zu nehmen.

Danach werden bestehende Vorgaben für die Unternehmen der Elektrizitätswirtschaft erfasst, die relevant sind für den Cyber-Bereich und Perspektiven angesichts der steigenden Cyber-Risiken geklärt.

1.2.1 Allgemeine Zuständigkeiten – Stromversorgungssicherheit

Energieversorgungssicherheit bedeutet, dass eine stets ausreichende und ununterbrochene Bereitstellung der nachgefragten Energie – unter Berücksichtigung der Wirtschaftlichkeit und Umweltverträglichkeit – gewährleistet ist.[32] Diese Definition lässt sich aus Art. 5 des Energiegesetzes (EnG) ableiten, welcher Leitlinien für die Energieversorgung regelt. Danach umfasst eine sichere Energieversorgung die ausreichende Verfügbarkeit, ein breit gefächertes Angebot sowie technisch sichere und leistungsfähige Versorgungssysteme.

Spezifisch für den Strombereich wird die Versorgungssicherheit dann als gewährleistet angesehen, wenn jederzeit die gewünschte Menge an Elektrizität mit der erforderlichen Qualität und zu angemessenen Tarifen bzw. Preisen erhältlich ist. Offensichtlich muss Cyber-Sicherheit und Resilienz daher im Rahmen der Versorgungssicherheit von Relevanz sein.

Der Schweizer Strommarkt zeichnet sich durch eine sehr hohe Zahl von Akteuren aus. Wie in dem Kapitel zur E-Survey genauer gezeigt wird, gibt es viele unterschiedliche Unternehmenstypen in dem Sektor. Die Gewährleistung einer sicheren Stromversorgung basiert folglich auf einem komplexen System.[33]

Die grundsätzliche Zuständigkeitsverteilung zwischen Behörden und den Unternehmen der Elektrizitätswirtschaft ergibt sich aus Art. 4 Abs. 2 EnG[34], wonach die Energieversorgung Sache der Energiewirtschaft ist. Bund und Kantone sorgen mit geeigneten staatlichen Rahmenbedingungen dafür, dass die Energiewirtschaft diese Aufgabe im Gesamtinteresse optimal erfüllen kann. Neben der Schaffung von geeigneten Rahmenbedingungen kommt dem Staat eine gewisse Verantwortung zum Eingreifen zu, falls die Unternehmen der Elektrizitätswirtschaft ihre Aufgaben nicht pflichtgemäss erfüllen (können). Einerseits kann der Bundesrat Massnahmen nach Art.9 Stromversorgungsgesetz (StromVG) ergreifen, um die mittel- bis langfristige Versorgung mit Elektrizität subsidiär sicherstellen zu können. Andererseits können im Rahmen der wirtschaftlichen Landesversorgung kurzfristige Massnahmen zur unmittelbaren Behebung vorübergehender Strommangellagen ergriffen werden.

Ein zentrales Element der Stromversorgung ist das Subsidiaritätsprinzip, wonach primär diejenigen Aufgaben hoheitlich geregelt werden, welche durch die Elektrizitätswirtschaft nicht selber im Gesamtinteresse wahrgenommen werden. Dies bedeutet ein grundsätzlicher Vorrang privater Massnahmen vor staatlichen Massnahmen.

Um einschätzen zu können, wann ein staatliches Eingreifen nötig ist, haben die ElCom und das BWL je ein Monitoring der Stromversorgungssicherheit implementiert. Die ElCom ist der Sektor-spezifische Regulator für die Elektrizitätswirtschaft und in dieser Rolle kommen ihr zwei wesentliche Zuständigkeiten zu, nämlich die Regulierung und die Überwachung des schweizerischen Elektrizitätsmarkts. Diesbezüglich Regulierung überwacht die ElCom die Einhaltung des StromVG, trifft die Entscheide und erlässt die Verfügungen, die für den Vollzug des StromVG und dessen Ausführungsbestimmungen notwendig sind (Art. 22 Abs. 1 StromVG). Im Bereich der Überwachung beobachtet und überwacht die ElCom die Entwicklung der Elektrizitätsmärkte im Hinblick auf eine sichere und erschwingliche Versorgung in allen

---

[32] Vgl. BFE, Grundlagen Energieversorgungssicherheit, Bericht vom 28. März 2012 zur Energiestrategie 2050, S. 7.

[33] Bundesamt für Energie (2017), Bericht - Zuständigkeiten im Bereich der Stromversorgungssicherheit zu Handen der UREK-N.

[34] Art.4 Abs.2 Der Bund und, im Rahmen ihrer Zuständigkeit, die Kantone und Gemeinden arbeiten für den Vollzug dieses Gesetzes mit den Organisationen der Wirtschaft zusammen.

Landesteilen (Art. 22 Abs. 3 StromVG). Die ElCom betreibt hierzu ein periodisches Monitoring der Stromversorgungssicherheit und veröffentlicht alle zwei Jahre einen entsprechenden Bericht. Dieser geht bislang nicht oder nur punktuell auf den Aspekt der Cyber-Sicherheit ein. Im Jahre 2019 hat die ElCom zudem einen ersten Bericht zum Thema Cyber-Sicherheit veröffentlicht[35].

Zeichnet sich mittel- oder langfristig eine erhebliche Gefährdung der inländischen Versorgungssicherheit ab, der die Unternehmen der Elektrizitätswirtschaft nicht aus eigener Kraft begegnen können, ist die ElCom verpflichtet, dem Bundesrat Vorschläge für Massnahmen nach Art. 9 StromVG zu unterbreiten (Art. 22 Abs. 4 StromVG). Die Vorschläge erfolgen im Einvernehmen mit dem BWL. Das BWL hingegen fokussiert das Monitoring der Stromversorgungssicherheit auf allgemeine Daten zur Beurteilung der Risiken für die Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen, sowie analysiert laufend die Versorgungslage.

Eine weitere zentrale Behörde auf Bundesebene für die Energieversorgungssicherheit ist das BFE. Das BFE erarbeitet und beurteilt energiewirtschaftliche Szenarien (Energieperspektiven) im Hinblick auf energiepolitische Massnahmen (Gesetze und Verordnungen). Die hauptsächlichen Zuständigkeiten des BFE im Bereich Stromversorgung sind folglich im Zusammenhang mit der Schaffung von geeigneten staatlichen Rahmenbedingungen gemäss Art. 4 Abs. 2 EnG zu berücksichtigen.

[35] Eidgenössische Elektrizitätskommission (2019), Bericht - Cyber-Sicherheit 2019.

Abbildung 5 stellt diese Abgrenzungen bezüglich Stromversorgungssicherheit dar und zeigt die Kompetenzen und Aufgabenbereiche der Akteure auf.

Energiepolitik / Energieperspektiven	**Stromversorgung**	**Gefährdung der Versorgungssicherheit**	**Strombewirtschaftung**
Energiepolitische Grundlagen für langfristige Versorgungssicherheit von Energie	**Bereitstellung und Übertragung von Strom**	**Sichere und erschwingliche Versorgung mit Elektrizität trotz der Vorkehrungen der Unternehmen der Elektrizitätswirtschaft mittel- oder langfristig erheblich gefährdet**	**Drohende oder bereits eingetretene, langandauernde Mangellage, welche die Wirtschaft nicht selbst beheben kann**
BFE erarbeitet Energieperspektiven und energiepolitische Massnahmen (Gesetze und Verordnungen) zuhanden BR und Parlament	**Energiewirtschaft** (Strombranche) zuständig für: - ausreichende Verfügbarkeit - Technisch sichere und leistungsfähige Versorgungssysteme	**ElCom** unterbreitet **BR** konkrete Vorschläge für Massnahmen - Strat. Netzausbau - Ausbau Erzeugung - Steigerung Effizienz	**WBF** Vorschlag an **BR** betr. Massnahmen nach Art. 28 LVG **BR** setzt **VEB** (Verordnung über die Elektrizitätsbewirtschaftung) in Kraft
EnG	EnG/StromVG	StromVG	LVG

Abbildung 5: Abgrenzungen bezüglich Stromversorgungssicherheit (UVEK, 2017, S. 14)

1.2.2 Bestehende Vorgaben mit Bezug zu Cyber-Sicherheit und Resilienz

Im Bereich der Energieversorgung und insbesondere der Stromversorgung bestehen derweil keine verpflichtenden und detaillierten Vorgaben bezüglich Cyber-Sicherheit. Vollständig unreguliert ist der Bereich der Cyber-Sicherheit in der Energieversorgung indes nicht. Es bestehen gewisse regulatorische, wenn auch stark fragmentierte Rahmenbedingungen, welche teilweise im Zusammenhang mit Vorgaben zur allgemeinen Versorgungssicherheit stehen.

In diesem Kapitel werden die zentralen, rechtlich verbindlichen Dokumente aufgeführt, beschrieben und miteinander verglichen. Dies ist jedoch keine rechtliche Analyse, sondern soll nur deskriptiv die Situation skizzieren. Es bestehen weitere Vorgaben, wie beispielsweise Risiko- und Schutzbedarfsanalysen, welche im Rahmen der SKI, der NCS oder Sektor-spezifischer Regulierungsvorhaben, wie z.B. der Einführung von intelligenten Messsystemen (Smart Meters) oder der Nutzung von Flexibilität (intelligente Steuerungen) durchgeführt wurden. Daneben existieren gewisse generelle Branchenrichtlinien. Diese werden aber nicht detailliert in diesem Kapitel erläutert, da sie meist nicht rechtlich bindend sind, sondern lediglich als ergänzende, unverbindliche Empfehlungen dienen. Eine Auflistung und Beschreibung dieser weiterführenden Dokumente ist in Anhang 3 und 4 zu finden. Grundsätzlich gehen diese Branchenrichtlinien auf sehr spezifische Thematiken ein und sind vor allem auf die Datensicherheit einzelner Technologien im OT-Bereich ausgelegt.

Zudem ist anzumerken, dass das Kernenergiegesetz (KEG) nicht berücksichtigt wird, da Nuklearanlagen nicht im Fokus des Berichts liegen. Nuklearanlagen müssen bereits gewisse Cyber-Auflagen einhalten und werden auch auf deren Einhaltung von der Eidgenössisches Nuklearsicherheitsinspektorat (ENSI) geprüft. Dies unterstreicht die Fragmentierung der bestehenden Vorgaben im Stromsektor, welche nachfolgend genauer begründet wird.

Bundesgesetz vom 17. Juni 2016 über die wirtschaftliche Landesversorgung *(Landesversorgungsgesetz*, LVG)

Das neue LVG, welches per 01.06.2017 in Kraft getreten ist, gibt dem BWL die Kompetenz, subsidiär präventive Massnahmen zur Sicherstellung der Energieversorgung umzusetzen. Vor diesem Hintergrund hat das BWL im Rahmen der Vorbereitungen auf eine unmittelbar drohenden Mangellage Aktivitäten hinsichtlich der Erarbeitung von Cyber-Standards für die Wirtschaft und insbesondere für die Stromversorgung übernommen. Dieser Vorgang basiert, wie in Tabelle 1 aufgeführt, auf einem Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit, welcher das NCSC und das WBF (das BWL gehört dem WBF an) in Zusammenarbeit mit anderen Fachämtern (für den Stromsektor das BFE) und Kantonen beauftragt bis Ende 2022 Lösungsoptionen für verpflichtende Sicherheitsstandards für die Betreiber von KI zu erarbeiten und Bericht zu erstatten.[36]

Energiegesetz vom 30. September 2016 *(EnG)*

Im Rahmen der bereits besprochenen allgemeinen Versorgungssicherheit (vgl. Kapitel 1.2.1), hält das EnG in Art. 6 fest, dass die Energieversorgung Sache der Energiewirtschaft ist. Der Bund und die Kantone sorgen für die erforderlichen Rahmenbedingungen. Art. 7 EnG hält Leitlinien fest, dass eine sichere Energieversorgung die jederzeitige Verfügbarkeit von ausreichend Energie, ein breit gefächertes Angebot, sowie technisch sichere und leistungsfähige Versorgungs- und Speichersysteme umfasst und dazu insbesondere auch der Schutz der KI einschliesslich der zugehörigen IKT gehört. Dies bezieht sich direkt auf die Gewährleistung der Cyber-Sicherheit und einer hohen Cyber-Resilienz. Weiter besagt Art. 8 EnG, dass Bund und Kantone mit der Energiewirtschaft zusammenarbeiten und sicherstellen, dass die Abläufe effizient sind und die Verfahren rasch durchgeführt werden.

Der Bereich IKT-Sicherheit[37] wurde mit der Energiestrategie 2050 nochmals ausdrücklich in Art. 7 Abs. 1 gestärkt. Das EnG statuiert demnach eine Verpflichtung aller Unternehmen der Energiewirtschaft zum Schutz ihrer IKT-Systeme. Gleichwohl findet sich keine eindeutige Definition der betroffenen Unternehmen, konkreter Massnahmen oder Vorgehensweisen. Es kann also durchaus angenommen werden, dass von dieser Vorgabe alle Unternehmen betroffen sind, die im Bereich Energie und insbesondere der Stromversorgung tätig sind, also auch Unternehmen, die z.B. sich vornehmlich auf den Bereich der Energiedienstleistungen konzentrieren. Es werden jedoch keine Aussagen über einen für den Bereich der Stromversorgungen empfohlenen oder verpflichtenden Mindeststandard für die Cyber-Sicherheit gemacht, auf welchen die NCS und die Expertenkommission hinwirken wollen.

Bundesgesetz vom 23. März 2007 über die Stromversorgung *(Stromversorgungsgesetz, StromVG)*

Das StromVG gilt für Elektrizitätsnetze, die mit 50 Hz Wechselstrom betrieben werden und fokussiert sich insbesondere auf Netzbetreiber und ihre Rechte und Pflichten. Darüber hinaus bestehen eher wenig Regelungen für andersartige Rollen des Stromversorgungssystems.

Gemäss Art. 8 StromVG sind die Netzbetreiber verpflichtet, ein «sicheres, leistungsfähiges und effizientes Netz» zu gewährleisten. Die Netzbetreiber müssen somit die erforderlichen Massnahmen treffen, damit sie den Endverbrauchern in ihrem Netzgebiet jederzeit die benötigte Menge an Elektrizität mit der erforderlichen Qualität und zu angemessenen Tarifen liefern können (Art. 6 Abs. 1 StromVG). Dies impliziert zwar auch Massnahmen zur IKT-Sicherheit, konkretisiert diese aber nicht. Es bestehen also für

---

[36] Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit (2018), Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit.

[37] Was grundsätzlich mit Cyber-Sicherheit gleichzusetzen ist (S. 6).

die Unternehmen der Energiewirtschaft keine weiteren expliziten Auflagen in Bezug auf die Handhabung von IKT-Risiken. Zudem findet sich auch keine Festlegung des Niveaus an Sicherheit, das erreicht werden soll.

Der ElCom obliegt gemäss StromVG Art.2 2 Abs. 3 die Überwachung der Einhaltung der Vorgaben aus dem StromVG. Sie beobachtet und überwacht dazu u.a. die Entwicklung der Strommärkte im Hinblick auf eine sichere und erschwingliche Versorgung in allen Landesteilen. Die Aufgaben der ElCom im Bereich der Cyber-Sicherheit sind insbesondere vor dem Hintergrund kaum vorhandener Vorgaben zu diesem Bereich im StromVG nicht vollständig klar und es gab insgesamt wenig Aktivitäten diesbezüglich. Im Anschluss an eine Befragung zur Cyber–Sicherheit[38] wurde bezüglich der Kosten für Sicherheitsmassnahmen kommuniziert, dass allfällige Kosten im Netzbereich anrechenbar in den Netzkosten sind, solange sie zur Sicherstellung der IKT-Sicherheit gemäss aktuellem Stand der Technik notwendig und effizient sind. Darüber hinaus wurde seitens ElCom die Erwartung kommuniziert, dass die entsprechenden Branchedokumente zum Thema Cyber Sicherheit auch umgesetzt werden. Produzenten, Aggregatoren, Bilanzgruppen und andere Unternehmen der Energiewirtschaft sind von dieser auf Netzbetreiber fokussierten Mitteilung nicht betroffen.

Stromversorgungsverordnung vom 14. März 2008 *(StromVV)*

Das BFE ist gemäss StromVV Art. 5 Abs. 6 befugt «technische und administrative Mindestanforderungen an ein sicheres, leistungsfähiges und effizientes Netz festlegen» oder in technischen Richtlinien zu konkretisieren. Ob die rechtliche Grundlage für das BFE hingegen, in Bezug auf den integralen Schutz des Netzes, sowie von Produktions- und Verbrauchsanlagen ausreichend ist, verbleibt zu prüfen. Es bestehen derzeit noch keine einschlägigen und für den Stromsektor übergreifenden Bestimmungen. Im Allgemeinen wurde diese Möglichkeit bisher nicht seitens des BFE in Anspruch genommen.

Im Bereich der intelligenten Messsysteme (Smart Meter) bestehen gewisse Vorgaben in Art. 8a und in Art. 8b StromVV gibt es eine konkrete Bestimmung, welche auf die Verpflichtung eines Branchenstandards im Bereich der Datensicherheit der intelligenten Messgeräte verweist.[39] Es dürfen somit nur Smart Meter und Kommunikationssysteme verwendet werden dürfen, die vorgängig eine Datensicherheitsprüfung durchlaufen und die entsprechende Zertifizierungen erreicht haben. Gemäss Anhang 1 des Metering Code Schweiz des VSE müssen die Hersteller von intelligenten Messsystemen ihr Produkt also bei einer akkreditierten Prüfstelle, hier der Konformitätsbewertungsstelle des Eidgenössischen Institut für Metrologie (METAS), zertifizieren lassen. Die Prüfmethodologie wurde durch den VSE und den Verein Smart Grid Industrie Schweiz (Swissmig) erarbeitet und publiziert. Sie fokussiert jedoch auf die Gerätschaften im intelligenten Messsystem, wie die elektronischen Zähler selbst (Smart Meter), die Kommunikationslösungen und die Schnittstellen zu den nachgelagerten Systemen. Bezüglich der Integration des intelligenten Messsystems in die Systemlandschaft der Netzbetreiber und Dienstleister sowie zum Betrieb ist ein freiwilliger Standard einschlägig (siehe folgend).

Weiter müssen gemäss Art. 6 Abs. 2 StromVV alle Netzbetreiber der ElCom jährlich gewisse Kennzahlen zur Versorgungsqualität einreichen, wie die durchschnittliche Unterbrechungsdauer («Customer Average Interruption Duration Index», CAIDI), die durchschnittliche Nichtverfügbarkeit des Systems («System Average Interruption Duration Index», SAIDI) und die durchschnittliche Unterbrechungshäufigkeit («System Average Interruption Frequency Index», SAIFI). Dies kann indirekt als eine Überwachung betreffend Cyber-Sicherheit verstanden werden, da diesbezüglich ungenügende Massnahmen

---

[38] Eidgenössische Elektrizitätskommission (2019), Bericht - Cyber-Sicherheit 2019.

[39] Vgl. Richtlinien für die Datensicherheit von intelligenten Messsystemen für Zertifizierung und Betrieb von intelligenten Messsysteme vom VSE.

die Kennzahlen beeinflussen würden. Jedoch sind diese Kennzahlen nur im Falle eines bereits stattgefundenen, sowie tatsächlich detektieren Vorfalls beeinträchtigt.

Freiwillige Mindeststandards für Cyber-Sicherheit

Im Rahmen seiner Tätigkeit in der NCS 2014-2018 und basierend auf dem LVG veröffentlichte das BWL einen freiwilligen «Minimalstandard zur Verbesserung der IKT-Resilienz» (IKT Minimalstandard), welcher im Kapitel der E-Survey genauer vorgestellt wird. Grundsätzlich basiert der IKT Minimalstandard auf dem amerikanischen «NIST Cybersecurity Framework»[40] und dient als Empfehlung und mögliche Richtschnur zur Verbesserung der allgemeinen IKT-Resilienz. Wo sinnvoll, wird der IKT Mindeststandard durch weitere international anerkannte Industriestandards, wie beispielsweise ISO/IEC 2700x[41] oder NIST Guide to Industrial Control Systems (ICS) Security, ergänzt.

Der Standard empfiehlt zum ersten Mal ein einheitliches, aber nicht verpflichtendes, Regelwerk, wie die Cyber-Sicherheit zu gewährleisten ist. Er richtet sich primär an die Betreiber von KI, ist aber für jedes Unternehmen anwendbar.

Der Standard ermöglicht einen vergleichsweise einfachen Einstieg in die Thematik, da grundlegende Elemente klar ausgelegt werden, und gewährleistet aber trotzdem ein relativ hohes Schutzniveau. Diese allgemeinen Vorgaben müssen jedoch auf den jeweiligen Sektor angepasst werden, damit ein höherer (technischer) Detaillierungsgrad erarbeitet werden kann. Zudem kann so auf Sektor-spezifische Gegebenheiten Rücksicht genommen werden.

Weiter publizierte der Branchenverband VSE in Zusammenarbeit mit dem BWL ein «Handbuch Grundschutz für Operational Technology» (2018), welches unverbindliche Massnahmen beschreibt und empfiehlt, wie Energieversorgungsunternehmen die Cyber-Sicherheit ihrer Prozess- und Netzleittechnik nachhaltig gewährleisten können und wendet sich an Personen, die in der Gesamtverantwortung der Sicherheit von Prozess- und Leitsystemen der Energieversorgung (Produktion und Netz) stehen. Diese Branchenrichtlinie übernimmt beinahe deckungsgleich den IKT Minimalstandard des BWL. Jedoch werden in dem Handbuch keine direkte Querverweise auf international, anerkannte Standards aufgeführt. Das Handbuch beruht jedoch auf dem IKT Standard (BWL), welcher wiederum auf internationalen Standards aufgebaut wurde, weshalb die Standards implizit berücksichtigt sind. Der Umsetzungsgrad obliegt jedem Netzbetreiber der Netzebenen 1 bis 4 resp. den Betreibern der Energieerzeugungsanlagen.

Letztlich publizierte der Branchenverband VSE zudem im Rahmen der Arbeiten zu den Sicherheitsanforderungen und zur Prüfmethodologie der intelligenten Messsysteme ebenfalls eine Branchenrichtlinie, wie diese intelligenten Messsysteme in die Systemlandschaft des jeweiligen Unternehmens, zumeist Netzbetreibers, zu integrieren und dort zu betreiben sind[42]. Diese betrieblichen Anforderungen sind in dem Metering Code Schweiz Anhang 2 des VSE zu finden und können mit dem OT-Handbuch verlinkt werden. Die Branchenrichtlinie ist im Gegensatz zu dem Metering Code Schweiz Anhang 1 des VSE nicht Gegenstand des Zertifizierungsverfahrens, sondern freiwilliger Natur.[43] Grundsätzlich bestehen

---

[40] Der NIST Framework wurde durch das US-amerikanische National Institute of Standards and Technology (NIST) entwickelt und gibt ein freiwilliges Rahmenwerk für Unternehmen zum organisatorischen und technischen Umgang mit Cyber-Risiken vor. Für mehr Informationen: https://www.nist.gov/cyberframework

[41] Die ISO/IEC 27000-Reihe ist eine Reihe von Standards zur Informationssicherheit. Herausgegeben werden Normen von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC). Die Standards werden in einem späteren Teil des Berichts erläutert.

[42] VSE, Swissmig (2018), Branchenempfehlung Strommarkt Schweiz. Richtlinien für die Datensicherheit von intelligenten Messsystemen, Anhang 4 Betriebliche Anforderungen an intelligente Messsystem für die Datensicherheit.

[43] Zur Klärung: Metering Code Anhang 1 ist relevant für die Lieferanten/Hersteller von Smart Metern. Metering Code Anhang 2 betrifft hingegen alle Smart Meter-Akteure.

beide Anhänge jedoch auf den gleichen Referenzdokumenten, insbesondere ISO27001/2 und NIST, weshalb zwischen Anhängen kein Widerspruch bestehen sollte.

Analyse zu bestehenden Vorgaben betreffend Cyber-Sicherheit und Resilienz

Es bestehen gewisse rechtlich verbindliche, aber fragmentierte und nicht unbedingt aufeinander abgestimmte oder nicht zwingend auf Cyber-Sicherheit fokussierte Auflagen und Pflichten. Konkret bestehen Vorgaben für:

- gewisse Unternehmenstypen im Bereich IKT-Sicherheit (StromVG für Netzbetreiber);
- die Cyber-Sicherheit einzelner Produkte (Branchenrichtlinie für die Datensicherheit der intelligenten Messgeräte gemäss StromVV, vgl. Anhang 4); oder
- generelle Massnahmen für die Stärkung der IKT-Sicherheit, welche aber unklar ausgelegt sind (EnG mit keinen konkreten Aussagen oder weiterführenden Ausführungen).

Die beiden rechtlich unverbindlichen Dokumente, IKT Minimalstandard und OT-Handbuch, sind zwar beide entlang des NIST-Frameworks in Verbindung mit weiteren anerkannten Standards und Frameworks aufgebaut, jedoch ist der Fokus des OT-Handbuchs auf OT-Sicherheit ohne die explizite Berücksichtigung von IT-Sicherheit zu kritisieren. Für die Stärkung der Cyber-Sicherheit sind unbedingt beide Bereiche zu sichern, da nur so ein umfassender Schutz vor Cyber-Bedrohungen garantiert werden kann. Mit der fortschreitenden Konvergenz der IT- und OT-Systeme sind die Funktionsfähigkeit beider Bereiche absolut notwendig für die Versorgungssicherheit.[44]

Weiter scheinen die einzelnen Anforderungen und Massnahmen auf der Stufe der Branchenrichtlinien eher wenig aufeinander und auf den IKT Minimalstandard abgestimmt, insbesondere, wenn man die Dokumente zum OT-Grundschutz und zum Betrieb intelligenter Messsysteme betrachtet. Beispielsweise findet sich in dem OT-Handbuch kein Querverweis zu der Branchenrichtlinie, obwohl Smart Meter als kritische Technologie für OT-Sicherheit anerkannt werden. Dies ist darauf zurückzuführen, dass die Dokumente parallel erarbeitet wurden. Grundsätzlich sind die Dokumente insofern kompatibel, als dass sie auf den gleichen international anerkannten Standards basieren.

Die bisher bindenden Dokumente sind mehrspurig ausgelegt und regeln einzelne Details für spezifische Bereiche, was eine gesamtheitliche Herangehensweise an die Cyber-Sicherheit und Resilienz stark erschwert und gegebenenfalls zu Widersprüchen und zu vermeidbaren Risiken führt. Schliesslich kann mit diesem groben Flickwerk an kaum verbindlichen und unklaren Vorgaben nur ein kleiner Teilbereich der gesamten Cyber-Sicherheit abgedeckt werden.

Die Regelungen sind demnach stark fragmentiert, welches zu Unsicherheiten bei den Betreibern betreffend Implementierung von Art. 7 Abs. 1 EnG geforderten Stärkung der IKT-Systeme führt. Grundsätzlich orientieren sich die Unternehmen je nach Themenbereich an den relevanten Dokumenten. Beispielsweise fokussiert sich die Mitarbeiter, welche für SCADA-Systeme verantwortlich sind, an dem OT-Handbuch und die Mitarbeiter, welche für Smart Meter zuständig sind, an den spezifischen Smart Meter Dokumenten. Mit der fortschreitenden Integration von Smart Meter in die Verbrauchs- und Produktionssteuerung ist jedoch ersichtlich, dass diese Trennung zwischen den Themenbereichen schwindet und Smart Meter zunehmend als OT anerkannt werden.

Eine für die Gesamtheit der Unternehmen der Energiewirtschaft umfassende, klare und verpflichtende Vorgabe zu Mindeststandards ist dabei ausstehend. Entsprechend erscheinen weitere Regelungen zu einzelnen Technologien oder Teilbereichen bei dem schon heute kaum durchschaubaren Dickicht an

---

[44] IT-/OT-Konvergenz beschreibt die zunehmende Integration von Systemen der IT zur Nutzung datenzentrischer Berechnungen mit Systemen der OT für die Überwachung von Ereignissen, Prozessen und Geräten und zur Durchführung von Anpassungen in Konzern- und Industriegeschäftsbereiche (Energy Expert Cyber Security Platform (2017), Report - Cyber Security in the Energy Sector).

Empfehlungen oder unklaren Vorgaben kontraproduktiv. Die Abstimmung dieser Empfehlungen und Vorgaben wird dadurch immer schwieriger.

1.3 Zusammenfassung

Fazit Kapitel 1 Aktueller Stand – regulatorisches Umfeld Schweiz

In der Schweiz bestehen bereits gewisse Regelungen zur Sicherstellung der Energieversorgungssicherheit, jedoch treffen diese nur beschränkt auf den Cyber-Bereich zu.

Die NCS 2018-2022 und die SKI 2018–2022 wurden als sektorübergreifende Initiativen anerkannt und die zahlreichen Massnahmen, welche innerhalb dieser Strategien beschlossen worden, sind teils für den Stromsektor anwendbar. Vor allem Massnahmen 4 «Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage», 8 «Evaluierung und Einführung von Minimalstandards» und 9 «Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung» der NCS werden für die Erarbeitung des Zielbilds im Stromsektor relevant sein.

Weiter zeigte die Diskussion auf, dass zwar verschiedene Ansätze für Cyber-Sicherheitsrichtlinien im Strommarkt bestehen, es aber keine eindeutige, einheitliche Regelung gibt. Auflagen und Pflichten sind stark fragmentiert und entweder nur für gewisse Unternehmenstypen / Produkte / Teilbereiche der Cyber-Sicherheit anwendbar oder allgemein zu unklar ausgelegt.

Eine für die Gesamtheit der Unternehmen der Energiewirtschaft umfassende und verpflichtende Vorgabe zu Mindestanforderungen ist bisher ausstehend. Entsprechend erscheinen weitere Regelungen zu einzelnen Technologien oder Teilbereichen bei dem schon heute kaum durchschaubaren Dickicht an Empfehlungen oder unklaren Vorgaben kontraproduktiv.

2 Quervergleich des regulatorischen Umfelds im Ausland und der Schweiz

Das bisherige Kapitel stellte den aktuellen Zustand des regulatorischen Umfelds betreffend Cyber-Sicherheit und Resilienz des Schweizer Stromsektors dar.

In diesem Kapitel wird ein Quervergleich des regulatorischen Umfelds im Ausland und der Schweiz durchgeführt, damit die schweizerischen Entwicklungen in diesem Bereich international eingeordnet werden können.

Zunächst wird in auf die regulatorischen Entwicklungen in den Vereinigten Staaten von Amerika (USA) eingegangen. Die Wahl der USA ist damit zu begründen, dass das Land grundsätzlich als sehr fortgeschritten in diesem Bereich gilt.[45]

Danach wird die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) der Europäischen Union (EU) beschrieben, um nachfolgend einen ausführlichen Quervergleich vornehmen zu können. Die Wahl der EU als zweite Vergleichskategorie ist unter anderem durch die starke Vernetzung des Schweizer Markts mit den europäischen Märkten zu begründen.

Die Absicht dieses Kapitels ist schliesslich die Identifikation von möglichen Handlungsfeldern, welche in dem angestrebten Konzept zur Cyber-Sicherheit und Resilienz konkret angegangen werden können. Der Vergleich zielt keinesfalls darauf ab, die Anforderungen der USA oder EU in der Schweiz unverändert zu übernehmen und dient lediglich als zusätzliche Richtschnur.

[45] Barichella, Arnault (2018), Cybersecurity in the energy sector: a comparative analysis between Europe and the United States.

2.1 Regulatorische Entwicklungen in den Vereinigten Staaten von Amerika

In den USA müssen Elektrizitätsunternehmen äusserst umfangreiche und strenge Cyber-Sicherheitsvorgaben einhalten. In der Cyber-Sicherheit Strategie des U.S. Department of Energy[46] werden vier entscheidende Prinzipien im Rahmen dieses Regulierungsbereich vorgegeben:

- «One Team, One Fight»: Im Sektor dürfen aufgrund der starken Vernetzung keine «weak links» bestehen.
- Employment of risk management methodology: Ein risikobasierter Ansatz berücksichtigt die dynamische Cyber-Bedrohungslage und erlaubt eine Priorisierung der Massnahmen entlang den wesentlichen Risiken.
- Prioritized planning and resourcing: Das Budget des U.S. Department of Energy beabsichtigt die Ausgaben, welche für die interne Stärkung der Cyber-Sicherheit benötigt sind, zu erhöhen.
- Enterprise-wide collaboration: Analog zu dem ersten Prinzip, wird die Zusammenarbeit hier insbesondere auf den Wissensaustausch betreffend Best Practices und allfälligen Cyber-Sicherheitsvorfällen[47] hervorgehoben.

Während das U.S. Department of Energy die strategische Richtung für das regulatorische Umfeld vorgibt, gibt die North American Electric Reliability Corporation (NERC) allen Unternehmen je nach Branche verbindliche «cybersecurity guidelines» vor.[48] Grundsätzlich folgen diese einem «security in depth» und «defense in breadth» Ansatz, was bedeutet, dass die Cyber-Anforderungen sehr detailliert und weitreichend ausgelegt sind. Beispielsweise muss jeder Betrieb einen ausführlichen Vorfallsreaktionsplan (engl. incident response plan) nachweisen können und das Personal, je nach Zugangsberechtigung zu kritischen Anlagen, regelmässig gemäss einem standardisierten Trainingsplan schulen.

Insbesondere kritische Infrastrukturen müssen gemäss der North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) äusserst strikte Cyber-Sicherheitsstandards erfüllen. Bei Nicht-Einhaltung können mehrere Millionen Dollar pro Tag als Strafe anfallen.[49]

Im Jahr 2020 hat der U.S. Kongress am American Energy Innovation Act gearbeitet, welcher zahlreiche Bestimmungen zur Cyber-Sicherheit enthält. Damit soll die Cyber-Sicherheit der nationalen Energieinfrastruktur durch öffentlich-private Partnerschaften gestärkt, Anreize für Cyber-Sicherheitsinvestitionen geschaffen und die Entwicklung von fortschrittlichen Cyber-Sicherheitstechnologien unterstützt werden. Es ist unwahrscheinlich, dass diese Gesetzgebung vor dem Ende dieses Kongresses verabschiedet wird, aber es ist zu erwarten, dass in 2021 ähnliche legislative Massnahmen beschlossen werden.

Da die Schweiz bislang eher einem generellen und nicht sehr ausführlichen Ansatz gefolgt ist, scheint die amerikanische Herangehensweise als zu spezifisch, welches den späteren Fokus auf die EU in diesem Bericht zusätzlich bekräftigt. Ein Angleichen an das amerikanische, detailliertere Regulierungssystem erscheint für die Schweiz vor dem Hintergrund der bisher eher fragmentierten bzw. fehlenden Vorgaben als zu ambitioniert.

---

46 U.S. Department of Energy (2018), Cybersecurity Strategy 2018-2020.

47 Hier wird besonders das fortschrittliche Warnsystem der North American Electric Reliability Corporation (NERC) hervorgehoben, welches alle Versorgungsunternehmen bei allfälligen Cyber-Vorfällen alarmiert.

48 Barichella, Arnault (2018), Cybersecurity in the energy sector: a comparative analysis between Europe and the United States.

49 Barichella, Arnault (2018), Cybersecurity in the energy sector: a comparative analysis between Europe and the United States.

2.2 Regulatorische Entwicklungen innerhalb der EU

Der Quervergleich mit der EU und spezifisch der NIS-Richtlinie wird durchgeführt, weil:

- die Schweiz eng in das europäische Energiesystem eingebunden ist. Dies gilt insbesondere für den Stromsektor. Die umfassende internationale technische und organisatorische Vernetzung des Stromsystembetriebs bedeutet wechselseitig starke Abhängigkeiten; die Sicherheit des Schweizer Stromsystems und ihrer Netze hat einen wesentlichen Effekt auf jene der EU. Kaskadeneffekte – wobei Probleme in einem Teil des Netzes leicht auf andere übergreifen können (S. 13) – erklären die Besorgnis, dass ein grossflächiger «Blackout» eintreten könnte; eine hohe Cyber-Sicherheit bedeutet auch eine hohe Versorgungssicherheit.
- die Verpflichtungen innerhalb EU auch als Best-Practices für die Schweiz angesehen werden können, da diese konkret und umfassend definiert sind, sowie, wie in Abbildung 6 verdeutlicht wird, bereits europaweit umgesetzt und gute Erfahrungen gesammelt wurden;
- es angenommen werden kann, dass die EU darauf Bedacht war, ihre Vorgaben international anzupassen und daher die Verpflichtungen genug weitreichend und relevant sind;
- Wie sich später in diesem Kapitel noch zeigen wird, die Logik der NIS-Richtlinie grundsätzlich mit jener der NCS übereinstimmt und die Massnahmen sich teilweise direkt überschneiden.

Die untenstehende Abbildung zeigt, dass die meisten europäischen Länder die NIS-Richtlinie umgesetzt haben. Die Schweiz ist eines der wenigen Länder, welche noch keine umfassenden verbindlichen Vorgaben für Cyber-Sicherheit an den Stromsektor abgegeben hat.

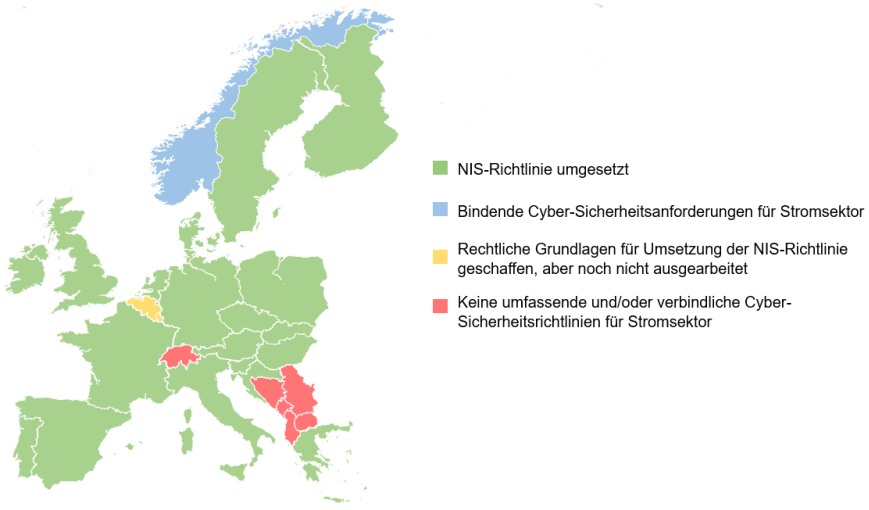


Abbildung 6: Europäischer Vergleich betreffend bindenden Sicherheitsanforderungen und Meldepflichten[50]

Dieser Vergleich bedeutet keinesfalls, dass die Anforderungen der EU für die Schweiz und insbesondere den Schweizer Stromsektor unverändert übernommen werden sollten. Aufgrund der oben aufgeführten Punkte erscheint jedoch ein angemessenes Angleichen an die Massnahmen der umliegenden Staaten und an die dafür grundlegenden regulatorischen Entwicklungen empfehlenswert. Ein Alleingang der Schweiz diesbezüglich und auch aufgrund gleichen Herausforderungen ist kaum angemessen bzw. wirtschaftlich nicht umsetzbar.

[50] Eigene Darstellung basierend auf Angaben in Bird & Bird (2020), Developments on NIS Directive in EU Member States.

Nachfolgend werden die Massnahmen der NIS-Richtlinie mit dem aktuellen Stand der Handlungsbereiche in der Schweiz gemäss bisherigen regulatorischen Erkenntnissen in Kapitel 1 durchgeführt. Ziel ist es, konkrete Handlungsfelder insbesondere gemäss dem aktuellen Umsetzungsstand der NCS 2018-2022 im Schweizer Stromsektor zu identifizieren.

2.2.1 Einführung zur Richtlinie Netz- und Informationssicherheit (NIS) der EU

Das Ziel der NIS-Richtlinie ist es ein gleichmässig hohes Sicherheitsniveau von Netz- und Informationssystemen in der gesamten EU zu erreichen.

Konkret strebt die NIS-Richtlinie drei Hauptziele an:

- erhöhte Kapazitäten im Bereich der Cyber-Sicherheit auf nationaler Ebene;
- verstärkte Zusammenarbeit auf EU-Ebene; und
- Verpflichtungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste in den Bereichen Risikomanagement und Meldung von Sicherheitsvorfällen.

Die Richtlinie stellte zur Erreichung dieser Ziele fünf Massnahmen an die EU- Mitgliedsstaaten:

1. die Pflicht für alle Mitgliedstaaten, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen;
2. die Schaffung einer Kooperationsgruppe, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten zu unterstützen und zu erleichtern und Vertrauen zwischen ihnen aufzubauen;
3. die Schaffung eines Netzwerks von Computer-Notfallteams (Computer Security Incident Response Team (CSIRT)[51] Netzwerk), um zum Aufbau von Vertrauen zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern;
4. Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste;
5. die Pflicht für die Mitgliedstaaten, nationale zuständige Behörden, zentrale Anlaufstellen, ein «Single Point of Contact (SPoC)» und CERTs mit Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen zu benennen.

Diese Massnahmen sind bindend und mussten von den Mitgliedsstaaten bereits bis Mai 2018 umgesetzt werden. Die Schweiz ist von dieser Pflicht ausgenommen. Die NIS-Richtlinie definiert zusätzlich gewisse Kriterien, welche bei der Umsetzung der einzelnen Verpflichtungen zu berücksichtigen sind. Diese Kriterien werden in der nachfolgenden Diskussion als Leitfäden genutzt, damit geprüft werden kann, ob die Schweiz und insbesondere der Schweizer Stromsektor die Massnahmen einhalten würde.

Praxisbeispiele wie Frankreich und Deutschland, die die NIS-Richtlinie implementiert haben und auf die bei Massnahmen oder Instrumenten Bezug genommen wird, sind in Anhang 5 angefügt.

---

[51] Wie in Kapitel 1.1.1. angemerkt, werden CSIRT und CERT in diesem Bericht synonym verwendet.

Derzeit wird die NIS-Richtlinie bereits wieder überarbeitet (NIS2), um die Richtlinie an die aktuellen Bedürfnisse anzupassen und diese zukunftssicher zu machen. Im Dezember 2020 wurde ein erster Entwurf für NIS2-Richtlinie von der Europäischen Kommission publiziert.[52]

Grundsätzlich werden die oben genannten Massnahmen auf eine grössere Anzahl von Sektoren ausgeweitet, wobei deren strategische Bedeutung für Wirtschaft und Gesellschaft zum Massstab genommen wird.

Der Entwurf zu NIS2 verlangt zudem:

- Stärkung der verbindlichen Sicherheitsanforderungen an Unternehmen, diese Massnahme wird neu als «Cybersecurity Risk Management Measures» definiert und wird auf zusätzliche Sektoren verglichen mit NIS1 erweitert;
- Explizite Berücksichtigung der Sicherheit von Lieferketten und Lieferantenbeziehungen,
- Konkretisierung der Meldepflicht anhand von genaueren Bestimmungen,
- Strengere Aufsichtsmassahmen betreffend Einhaltung der Sicherheitsanforderungen und Meldepflichten der betroffenen Unternehmen durch nationale Behörden,
- Verschärfung der Durchsetzungsanforderungen bei Nichteinhaltung der NIS von Mitgliedsstaaten; und
- Harmonisierung der Sanktionsregelungen in den Mitgliedstaaten.

Die grundlegende Struktur und Massnahmen bleiben somit bestehen, wenn auch die Anforderungen um einiges erhöht werden gegenüber der NIS1-Richtlinie.

Öffentliche Konsultationen zu dem Vorschlag fanden zwischen Juli und Oktober 2020 statt. Ein zusammenfassender Bericht der Europäischen Kommission hebt als Resultat hiervon hervor, dass rund 88.4% der Teilnehmer angegeben haben, dass Cyber-Bedrohungen seit 2016 zugenommen haben. Eine überwältigende Mehrheit sprach sich zudem für eine gemeinsame Regelung der Anforderungen auf EU-Ebene aus.[53]

Aktuell ist der Vorschlag zur NIS2-Richtlinie noch Gegenstand von Verhandlungen im Trilog, also zwischen dem Rat der EU, dem Europäischen Parlament und der Europäischen Kommission. Sobald der Vorschlag im Trilog angenommen ist, müssen die Mitgliedstaaten die NIS2-Richtlinie innerhalb von 18 Monaten umsetzen. Schliesslich muss die Europäische Kommission die NIS2-Richtlinie regelmässig überprüfen und 54 Monate nach Inkrafttreten erstmals über die Implementierung Bericht erstatten. Der nachfolgende Quervergleich basiert auf NIS1-Richtinie, da die genaue Auslegung der überarbeiteten Version noch nicht verankert ist und die fundamentalen Massnahmen grundsätzlich fortbestehen.

Generell ist die Überarbeitung der NIS1-Richtlinie im Rahmen der ebenso im Dezember 2020 neu vorgelegten Cyber-Sicherheitsstrategie der EU einzuordnen. Neben der Überarbeitung der NIS-Richtlinie schlägt die Kommission weiter vor, ein Netz von Sicherheitseinsatzzentren in der gesamten EU mithilfe künstlicher Intelligenz aufzubauen. Damit soll gewissermassen ein ‘cybersecurity shield' («Cyber-Sicherheitsschutzschild») erarbeitet werden, welches frühzeitige Signale für drohende Cyber-Angriffe zu erkennen und die entsprechenden Massnahmen zu ermöglichen soll, bevor Schäden verursacht werden.

---

[52] Europäische Kommission (2020a), Proposal for directive on measures for high common level of cybersecurity across the Union.

[53] Europäische Kommission (2021), Summary Report on the open public consultation on the Directive on security of network and information systems (NIS Directive).

2.2.2 Quervergleich der Massnahmen der NIS-Richtlinie mit dem aktuellem NCS-Umsetzungsstand im Schweizer Stromsektor

Nachfolgend wird ein Quervergleich zwischen den fünf NIS1-Massnahmen und dem aktuellen Stand der Handlungsfelder in der Schweiz gemäss bisherigen regulatorischen Erkenntnissen in Kapitel 1 durchgeführt.

EU NIS1 Massnahme # 1: Festlegung einer nationalen Strategie

Die NIS1-Richtlinie fordert für die Mitgliedstaaten eine nationale Strategie zur Gewährleistung der Sicherheit von Netz- und Informationssystemen als einen Rahmen mit strategischen Zielen und Prioritäten. Darauf basierend sollen angemessene Regulierungsmassnahmen bestimmt werden, mit denen ein hohes Sicherheitsniveau erreicht und aufrechterhalten werden soll. Die Strategie muss mindestens alle Sektoren abdecken, welche gemäss NIS1 Massnahme # 4 verpflichtende Sicherheitsanforderungen und Meldepflichten einzuhalten haben.

Die untenstehende Tabelle gibt die in der NIS-Richtlinie festgehaltenen Kriterien an, welche bei der Erarbeitung einer nationalen Strategie zu berücksichtigen sind und zeigt an, ob diese Kriterien in der Schweiz bereits erfüllt worden wären:

Tabelle 3: NIS1-Richtlinie - Kriterien für nationale Strategie

NIS1-Kriterien für nationale Strategie, Art. 7	Schweiz	Begründung
Festlegung von Zielen und Prioritäten. [NIS1 Art. 7 (1) a]		Vision und strategische Ziele in NCS festgelegt.
Definition von Steuerungsrahmen zur Erreichung dieser Ziele, einschliesslich der Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure. [NIS1 Art. 7 (1) b]		NCS Umsetzungsplan definiert diese Bereiche.
Bestimmung von Massnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung, einschliesslich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor. [NIS1 Art. 7 (1) c]		In mehreren Handlungsbereichen und Massnahmen der NCS berücksichtigt.
Aufstellung der Ausbildungs-, Aufklärungs- und Schulungsprogramme im Zusammenhang mit der nationalen Strategie. [NIS1 Art. 7 (1) d]		In mehreren Handlungsbereichen und Massnahmen der NCS berücksichtigt.
Angabe der Forschungs- und Entwicklungspläne im Zusammenhang mit der nationalen Strategie. [NIS1 Art. 7 (1) e]		In mehreren Handlungsbereichen und Massnahmen der NCS berücksichtigt.
Risikobewertungsplan zur Bestimmung von Risiken. [NIS1 Art. 7 (1) f]		Aus Basis der ersten NCS 2012-2017 wurden Risiko- und Schutzbedarfsanalysen in den kritischen Sektoren durchgeführt.
Liste der verschiedenen Akteure, die an der Umsetzung der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen beteiligt sind. [NIS1 Art. 7 (1) g]		NCS Umsetzungsplan definiert diese Bereiche auf Bundesebene.

Die Analyse zeigt auf, dass die Schweiz alle Kriterien der Massnahme #1 der NIS1-Richtlinie erfüllt.

EU NIS1 Massnahme # 2: Errichtung einer Kooperationsgruppe

Diese zweite Massnahme gemäss Art. 11 der NIS1-Richtlinie ist nicht direkt relevant für die Schweiz, da sich die Kooperationsgruppe sich aus Vertretern der MS, der Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) zusammensetzt. Deshalb wurde im Rahmen dieses Berichts auf die Ausarbeitung der entsprechenden Kriterien verzichtet.

Das Ziel der Kooperationsgruppe ist die Unterstützung der strategischen Zusammenarbeit und des Informationsaustausches zwischen den Mitgliedsstaaten, um so auch das Vertrauen zwischen ihnen aufzubauen und die Kompetenzen anzugleichen. Aufgaben der Gruppe sind unter anderem:

- Austausch von Informationen und bewährten Verfahren zu Sensibilisierung und Schulung;
- Austausch von Informationen und bewährten Verfahren zu Forschung und Entwicklung bezüglich der Sicherheit von Netz- und Informationssystemen;
- Sammlung von Informationen über bewährte Verfahren bei Risiken und Sicherheitsvorfällen.

Jeweils im Abstand von eineinhalb Jahren legt die Gruppe einen öffentlichen Bericht vor, in dem der Nutzen der Zusammenarbeit beurteilt wird. Der Bericht wird der Kommission als Beitrag zur Überprüfung der Anwendung der Richtlinie übermittelt.

Die Schweiz als Nicht-Mitgliedstaat der EU ist in diese Arbeiten nicht einbezogen, zielt aber gemäss NCS Massnahme 25 «Aktive Mitgestaltung und Teilnahme an Prozessen der Cyber-Aussensicherheitspolitik» darauf ab, die Entwicklungen in der EU zu verfolgen. Der NCS Umsetzungsplan legt fest, dass Prozesse und Zuständigkeiten für Beobachtung der EU-Entwicklungen und allfällige Beteiligungen bis Ende 2021 erarbeitet werden sollen. Es ist deshalb zu dem Erfassungszeitpunkt dieses Berichts unklar, ob und in welchem Rahmen die Schweiz sich an dieser Kooperationsgruppe beteiligen kann und wird.

EU NIS1 Massnahme # 3: Netzwerk von Computer-Notfallteams

Um zum Aufbau von Vertrauen zwischen den Mitgliedsstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern, wurde ein zentrales CERT-Netzwerk mit Vertretern der CERTs der EU-Mitgliedsstaaten und dem CERT-EU[54] geschaffen.

Da die Schweiz kein EU- Mitgliedsstaat ist, ist auch diese Verpflichtung nicht direkt relevant. Deshalb wurde im Rahmen dieses Berichts auf die Ausarbeitung der entsprechenden Kriterien verzichtet. Jedoch unterstreicht die Verpflichtung die Wichtigkeit von einem internationalen Wissensaustausch betreffend aktuellen Cyber-Gefahren. Das nationale Schweizer CERT (GovCERT)[55], welches dem NCSC untersteht, anerkennt diese Anforderungen und ist Mitglied des Forum of Incident Response and Security Teams (FIRST)[56] und dem European Government CERTs (EGC)[57]. Das Schweizer GovCERT unterhält weitere Beziehungen zu anderen CERTs und GovCERTs auf der ganzen Welt, hat aber kein institutionalisiertes Verhältnis zu dem zentralen EU-CERT Netzwerk.

---

54 Das CERT-EU ist für die Cyber-Sicherheit der EU-Institutionen zuständig.

55 Vgl. Kapitel 1.1.1 Nationale Strategie zum Schutz vor Cyber-Risiken 2018-2022 (NCS).

56 Globales Netzwerk von individuellen CERTs mit über 220 Mitgliedern aus 42 Ländern.

57 Informeller Zusammenschluss europäischer Regierungs-CERTs.

EU NIS1 Massnahme # 4: Verpflichtende Sicherheitsanforderungen und Meldepflicht

Im Rahmen der NIS1-Richtlinie müssen ermittelte Betreiber wesentlicher Dienste angemessene Sicherheitsvorkehrungen treffen und der jeweiligen nationalen Behörde gravierende Cyber-Sicherheitsvorfälle melden. Diese Massnahme ist an die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste gerichtet.

Betreiber wesentlicher Dienste können private Unternehmen oder öffentliche Einrichtungen sein, welche in den Bereichen Gesundheitswesen, Verkehr, Energie, Banken und Finanzmarktinfrastrukturen, digitale Infrastruktur und Wasserversorgung eine wichtige Rolle bei der Gewährleistung der Versorgungssicherheit spielen. Als Anbieter digitaler Dienste können die folgenden Organisationen kategorisiert werden: Online-Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze - diese sind aufgrund des Fokus dieses Berichts auf den Strommarkt nicht weiter relevant.

Die Definition von Betreibern wesentlicher Dienste liegt im Kompetenzbereich der Mitgliedsstaaten und musste individuell auf Mitgliedsstaaten-Ebene bis im November 2018 ermittelt werden. Lediglich im Anhang der NIS1-Richtlinie findet sich eine grobe Übersicht betreffend Arten von Einrichtungen, welche für diese Kategorisierung verwendet werden können.

Für den Teilsektor Elektrizität werden die folgenden Unternehmensarten benannt:

- Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 35 der Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates (1), die die Funktion „Versorgung“ im Sinne des Artikels 2 Nummer 19 jener Richtlinie wahrnehmen;
- Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/72/EG; und
- Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/72/EG.

Als Praxisbeispiele definierte zum Beispiel Frankreich sieben verschiedene Kriterien und teilte die Betreiber zentral als KI ein, während Deutschland ein einziges Kriterium vorgab (Versorgungsgrad beträgt 500.000 oder mehr versorgte Personen) anhand von welchem sich die Betreiber eigenständig als KI identifizieren mussten. Anhang 5 führt die beiden Praxisbeispiele weiter aus.

Ziel dieser Massnahme der NIS1-Richtlinie ist es, eine Kultur des Risikomanagements zu fördern und sicherzustellen, dass die gravierendsten Sicherheitsvorfälle gemeldet werden. Beide dieser Ziele überschneiden sich stark mit der NCS, da das Handlungsfeld Standardisierung / Regulierung anhand von Massnahmen 8 «Evaluierung und Einführung von Minimalstandards» und 9 «Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung» auf die Verankerung dieser Vorgabe in der Schweiz abzielt.

Nachfolgend werden die drei Artikel der NIS1-Richtlinie, welche diese vierte NIS1-Massnahme angehen, aufgelistet und deren konkrete Anforderungen mit dem Umsetzungsstand in der Schweiz verglichen.

Tabelle 4: NIS1-Richtlinie - Kriterien für Sicherheitsanforderungen

NIS1-Kriterien für Sicherheitsanforderungen, Art . 14	Schweizer Stromsektor	Begründung
Verpflichtung der KI Betreiber zu geeigneten und verhältnismässigen technischen und organisatorischen Massnahmen. [NIS1 Art. 14 (1)]	⊗	Für den Stromsektor wurden noch keine konkreten verpflichtenden IKT-Sicherheitsanforderungen festgelegt. Einzig im Bereich der intelligenten Messsysteme (Smart Meter) findet sich in Art. 8b StromVV eine Bestimmung. Dies ist jedoch sehr spezifisch für intelligente Messsysteme und behandelt nur einen kleinen Teilaspekt der Cyber-Sicherheit.
Berücksichtigung des Stands der Technik. [NIS1 Art. 14 (1)]	⊗	Für den Stromsektor wurden noch keine konkreten verpflichtenden IKT-Sicherheitsanforderungen festgelegt, da grundsätzlich, gemäss EnG Art. 7, die Verantwortung für IT-Sicherheit bei dem Betreiber liegt.
Dem bestehenden Risiko angemessen. [NIS1 Art. 14 (1)]	⊗	Siehe oben.

Tabelle 5: NIS1-Richtlinie - Kriterien für Meldepflicht

NIS1-Kriterien für Meldepflicht, Art . 14	Schweiz Stromsektor	Begründung
Erhebliche Auswirkungen auf die Verfügbarkeit der bereitgestellten wesentlichen Dienste werden unverzüglich gemeldet. [NIS1 Art. 14 (3)]		Es besteht für Netzbetreiber bereits eine nicht-cyberspezifische Form der Meldepflicht an die ElCom (Art. 8 Abs. 3 StromVG), welche auf «ausserordentliche Ergebnisse» beschränkt ist. Der Bundesrat hat sich im Dezember 2020 für eine Meldepflicht für kritische Infrastrukturen bei Cyber-Angriffen ausgesprochen. Bis Ende 2021 wird eine Vernehmlassungsvorlage ausgearbeitet, welche die rechtlichen Grundlagen für eine Meldepflicht schaffen soll.
Meldungen müssen die Informationen enthalten, die es der zuständigen Behörde oder dem CERT ermöglichen, zu bestimmen, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat. [NIS1 Art. 14 (3)]		Siehe oben.
Zur Feststellung des Ausmasses der Auswirkungen eines Sicherheitsvorfalls werden insbesondere folgende Parameter berücksichtigt: - Zahl der von der Unterbrechung der Erbringung des wesentlichen Dienstes betroffenen Nutzer; - Dauer des Sicherheitsvorfalls; - geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet. [NIS1 Art. 14 (4)]		Siehe oben.
Weiterreichen der erhaltenen Meldung an die zuständige Behörde oder das CERT den bzw. die anderen betroffenen MS, sofern der Vorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in jenem Mitgliedstaat hat. [NIS1 Art. 14 (5)]		Grundsätzlich werden freiwillige Meldungen bei Cyber-Vorfällen beim NCSC gesammelt und an internationale CERT-Netzwerke weitergereicht. Dies ist aber rechtlich nicht verankert.
Die zuständige Behörde oder das CERT stellt dem betroffenen Betreiber Informationen für die weitere Behandlung der Meldung, wie etwa der Sicherheitsvorfall bekämpft werden kann, zur Verfügung. [NIS1 Art. 14 (5)]		Bei freiwilligen Meldungen von Cyber-Vorfällen bietet das NCSC bei Bedarf weiterführende Informationen an. Diese Hilfestellung ist aber noch nicht umfassend institutionalisiert.
Die Öffentlichkeit kann über einzelne Sicherheitsvorfälle unterrichtet werden. [NIS1 Art. 14 (6)]		Hierfür konnte im Rahmen dieses Berichts keine Regelung identifiziert werden.

Die vorliegende Analyse zeigt, dass für den Schweizer Stromsektor noch keine verpflichtenden Massnahmen weder für Sicherheitsanforderungen noch für Meldepflichten verabschiedet wurden. Lediglich im Bereich der intelligenten Messsysteme (Smart Meter) findet sich, wie Kapitel 1.2.2 aufgezeigt, in Art. 8b StromVV eine Bestimmung, welche einen Branchenstandard im Bereich der Datensicherheit der elektronischen Geräte und ihrer kommunikationstechnischen Anbindung als verpflichtend bezeichnet. Dies ist aber nur ein kleines Fragment in Bezug auf Cyber-Sicherheit. Die Vorgabe zur Verankerung von verpflichtenden Cyber-Sicherheitsanforderungen ist also bei Weitem nicht erfüllt. Bezüglich der Meldung von Cyber Vorfällen besteht in der Schweiz eine grundsätzliche Meldepflicht bei ausserordentlichen Sicherheitsvorfällen, jedoch sind diese nicht cyberspezifisch definiert. Zudem ist unklar, welche Behörde letztlich bei Cyber-Vorfällen zuständig ist und was sie zu tun hat; NCSC, GovCERT und der ElCom kommen verschiedene Verantwortungen zu.

Mittlerweile hat der Bundesrat Grundsatzentscheide über die Einführung von Meldepflichten für KI gefällt.[58] In diesem Zusammenhang sind Sektor-spezifische Meldepflichten für den Stromsektor zu erwarten bzw. erscheinen unausweichlich.

Weiter wurden auch das BWL und NCSC in Zusammenarbeit mit den Fachämtern beauftragt, verpflichtende IKT-Sicherheitsstandards für KI zu erarbeiten.[59] Es dürften also alsbald erste Schritte zur Umsetzung dieser NIS1 Vorgaben unternommen werden.

[58] Bundesrat (2020), Medienmitteilung: Bundesrat spricht sich für eine Meldepflicht für kritische Infrastrukturen bei Cyberangriffen aus.

[59] Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit (2018), Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit.

Für die Verpflichtung zur Schaffung von Sicherheitsanforderungen wird zusätzlich in der NIS-Richtlinie in einem separaten Artikel festgelegt, wie deren Umsetzung und Durchsetzung bei den Betreibern von wesentlichen Diensten nachzuweisen ist:

Tabelle 6: NIS1-Richtlinie - Kriterien für Umsetzung und Durchsetzung

NIS1-Kriterien für Umsetzung und Durchsetzung, Art. 15	Schweiz Stromsektor	Begründung
Die Betreiber von wesentlichen Diensten sind dazu zu verpflichten, Informationen, welche für die Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlich sind, an die national zuständige Behörde einzureichen. [NIS1 Art.15 (2) a]	⊗	Da im Stromsektor noch keine Verpflichtungen betreffend Sicherheitsanforderungen aufgestellt wurden, findet entsprechend auch keine Überprüfung der Umsetzung statt.
Nachweise für die wirksame Umsetzung der Sicherheitsmassnahmen werden zur Verfügung gestellt stellen, wie etwa die Ergebnisse einer von der zuständigen Behörde oder einem qualifizierten Prüfer durchgeführten Sicherheitsüberprüfung, und im letztgenannten Fall die Ergebnisse der Überprüfung einschliesslich der zugrunde gelegten Nachweise der zuständigen Behörde zur Verfügung stellen. [NIS1 Art.15 (2) b]	⊗	Siehe oben.
Basierend auf den Ergebnissen der Sicherheitsprüfung kann die zuständige Behörde den Betreibern wesentlicher Dienste verbindliche Anweisungen zur Abhilfe der festgestellten Mängel erteilen. [NIS1 Art.15 (3)]	⊗	Siehe oben.

Da im Stromsektor noch keine Verpflichtungen betreffend Sicherheitsanforderungen aufgestellt wurden, findet entsprechend auch keine Überprüfung der Umsetzung statt.

Die NIS-Richtlinie fordert zudem, dass für eine einheitliche Implementierung der Sicherheitsanforderungen, die Mitgliedsstaaten europäische oder international anerkannte Normen und Spezifikationen, also Standards, für die Sicherheit von Netz- und Informationssystemen verwenden sollen.

Analog hat die Europäische Kommission eine Empfehlung zur Einführung und Verwendung von Normen zur Cybersicherheit im Energiesektor abgeben. In dieser Empfehlung werden zentrale Herausforderungen für die Cyber-Sicherheit im Energiesektor — Echtzeitanforderungen, Kaskadeneffekte und die Kombination älterer und modernster Technologien — dargestellt und wesentliche Schritte zur möglichst angeglichenen Umsetzung wichtiger Sicherheitsanforderungen identifiziert.[60]

[60] Empfehlung (EU) 2019/553 der Kommission vom 3. April 2019 zur Cybersicherheit im Energiesektor.

Diese ersten Schritte betreffend Normung im Energiesektor sollen weiter anhand öffentlicher Konsultationen der Europäischen Kommission von 2020-2023 ausgearbeitet werden.[61] Konkret soll ein Energie-spezifischer «Cybersecurity Network Code» etabliert werden. Sogenannte Netzkodizes wurden bisher von dem European Network of Transmission System Operators for Electricity (ENTSO-E)[62] erarbeitet werden aber demnächst gemeinsam und der European Union Distribution System Operator Entitiy (EUDE)[63] formuliert. Aufgrund der Zuständigkeiten von ENTSO-E und EUDE sind vor allem Übertragungsnetzbetreiber und Verteilnetzbetreiber im Fokus der Netzkodizes. Es existieren bereits zahlreiche Netzkodizes, welche unterschiedliche technische Aspekte regeln, um die Funktionsfähigkeit des internationalen Stromsektors zu garantieren. Beispielsweise wurde verbindlich festgelegt, wie und wann ein Netzbetreiber einspeisende Kraftwerke abregeln darf, um Spannung und Frequenz im Stromnetz stabil zu halten.

Somit werden die Vorgaben der NIS1 und zukünftig der NIS2 betreffend verbindlicher Sicherheitsanforderungen durch den «Cybersecurity Network Code» konkretisiert und auch international harmonisiert. Ein erster Entwurf für den «Cybersecurity Network Code» wird Mitte 2021 erwartetet.

Ein zentrales Dokument, welches von der Smart Grid Task Force Expert Group auf Anfrage der Europäischen Kommission vorgängig im Juni 2019 veröffentlicht wurde, zeigte erste mögliche Stossrichtungen für den «Cybersecurity Network Code» auf.[64] Die untenstehende Abbildung fasst die Vorschläge zusammen:

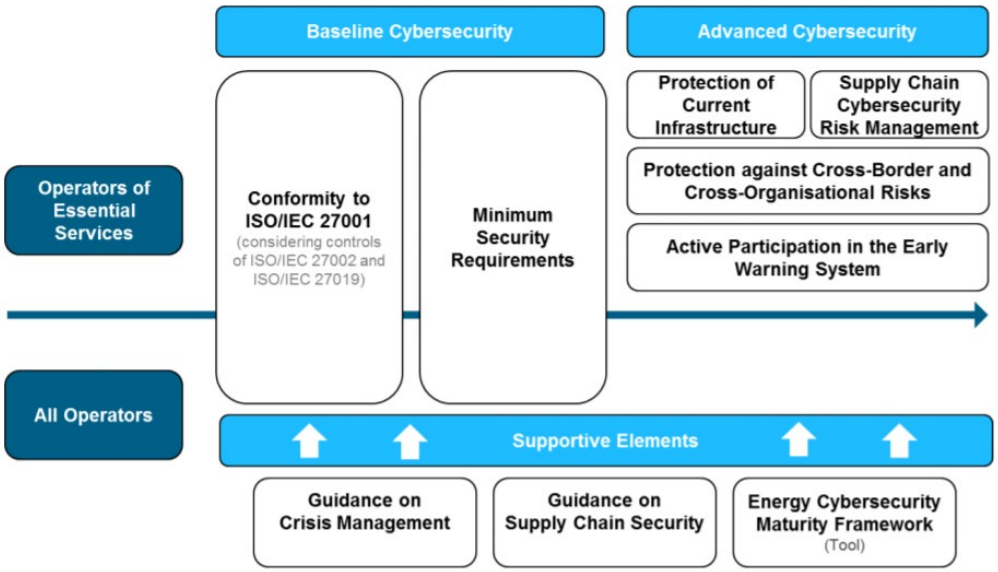


Abbildung 7: Empfehlung der Smart Grid Task Force Expert Group für Cybersecurity Network Codes (2019).

---

61 Europäische Kommission (2020b), Public consultation to establish the priority list of network codes.

62 ENTSO-E ist ein europäischer Verband in der alle Übertragungsnetzbetreiber Pflichtmitglieder sind. Swissgrid ist Mitglied von ENTSO-E.

63 EUDE wird voraussichtlich offiziell im Januar/Februar 2021 als europäischer Verband für Verteilnetzbetreiber gegründet.

64 Smart Grid Task Force Expert Group (2019) Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management.

Es zeigt sich, dass zwischen Betreibern von KI und anderen Betrieben unterschieden wird. Der Umfang der einzuhaltenden Vorgaben unterscheidet sich stark zwischen den beiden Unternehmenstypen, wobei alle zumindest ISO/IEC27001, sowie möglicherweise ISO/IEC27002 und ISO/IEC27019 einzuhalten und danach zertifizieren zu haben.[65] Die Betreiber von KI müssen darüber hinaus zusätzliche Massnahmen erfüllen, welches mit deren wesentlichen Kritikalität betreffend Versorgungssicherheit zu begründen ist. Entsprechend ist die Cyber-Bedrohungslage solcher Unternehmen meist höher als jene von nicht-KI Betreibern, da die Wahrscheinlichkeit eines Cyber-Angriffs sowie deren Auswirkungen bedeutend ist.

EU NIS1 Massnahme # 5: Zuständige Behörden und CERT

Damit die vorhergehenden Massnahmen umgesetzt werden können, verpflichtet Art. 8 und Art. 9 der NIS1-Richtlinie die Mitgliedsstaaten zur Ernennung von nationalen zuständigen Behörden, zentralen Anlaufstellen und nationalen CERTs.

Nationale zuständige Behörden überwachen die Anwendung der NIS-Richtlinie auf nationaler Ebene. Jeder Mitgliedsstaat muss eine oder mehrere für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörden benennen. Hier ist die Unterscheidung zwischen Sektor-spezifischen oder Sektor-übergreifenden Massnahmen relevant. Sektorübergreifend bedeutet, dass von allen KI unabhängig des Sektors die gleichen Sicherheitsanforderungen gefordert werden. Entsprechend ist meistens die national zuständige Behörde zentral aufgestellt, da die Umsetzung der Massnahmen aller KI Betreibern mit einer Behörde geregelt wird. Hingegen können die Sicherheitsanforderungen an die unterschiedlichen Sektoren angepasst werden, womit auf die sektoriellen Unterschiede zwischen den Betreibern Rücksicht genommen wird. Daher werden in diesem Modell meist mehrere national zuständige Behörden eingesetzt, welche die Sektor-spezifische Implementierung und korrespondierenden Zuständigkeiten reflektieren.

Die zentrale Anlaufstelle wird zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation für eine effektive Umsetzung der Richtlinie ernannt. Diese Verbindungsstelle, auch Single Point of Contact (SPoC) genannt, ist für die Koordinierung im Zusammenhang mit der Sicherheit von Netz-und Informationssystemen und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig. Jeder MS hat ungeachtet von Sektor-spezifischen regulatorischen Vereinbarungen eine zentrale Anlaufstelle für diese EU-weite Kooperation zu benennen.

Jeder Mitgliedsstaat hat zudem mindestens ein nationales CERT einzurichten. Das nationale CERT muss Mitglied des Netzwerkes für Computer-Notfallteams (vgl. NIS1-Massnahme # 3) sein. In der NIS1-Richtlinie werden keine Kriterien für den Aufbau des nationalen CERTs definiert.

Handelt es sich bei der zuständigen Behörde, der zentralen Anlaufstelle und dem CERT desselben Mitgliedstaats um getrennte Einrichtungen, so arbeiten sie bei der Erfüllung der in dieser Richtlinie festgelegten Pflichten zusammen.

In dem Schweizer Stromsektor zeigt sich das folgende Bild.

---

[65] Die ISO/IEC 27000-Reihe ist eine Reihe von Standards zur Informationssicherheit. Herausgegeben werden Normen von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC). Die Standards werden in einem späteren Teil des Berichts erläutert.

Tabelle 7: NIS1-Richtlinie - Kriterien für zuständige Akteure

Kriterien für zu ernennende Akteure, Art. 8 & 9	Schweiz Stromsektor	Begründung
Nationale zuständige Behörden [NIS1 Art. 8 (2 & 3)]		Auf Bundesebene wurde anhand des NCS Umsetzungsplans Verantwortlichkeiten für die Massnahmen festgelegt, aber die Zuständigkeiten für die Cyber-Sicherheit im Schweizer Stromsektor sind noch nicht klar definiert.
Zentrale Anlaufstelle [NIS1 Art. 8 (4)]		Das NCSC wurde kürzlich als nationale Anlaufstelle für alle Fragen mit Bezug zur Cyber-Sicherheit in der NCS festgelegt.
Nationales CERT [NIS1 Art. 9]		Das GovCERT agiert als nationales CERT der Schweiz. Laut Umsetzungplan für NCS Massnahme 4 muss die Bedrohungslage jedoch jeweils adressatengerecht aufbereitet werden und daher wäre eine zusätzliche, Sektor-spezifische Ausrichtung für die zielgerichtete Vorbereitung auf Sektor-spezifische Bedrohungsszenarien nützlich.

Die Einschätzung betreffend Kriterien für die Umsetzung und Durchsetzung der Sicherheitsanforderungen und Meldepflichten ergibt sich aus der Diskussion in Kapitel 1.2.2, wo dargelegt wurde, dass die Zuständigkeiten für die Cyber-Sicherheit in dem Schweizer Stromsektor noch nicht klar definiert sind. Die bisherigen Aktivitäten finden meist mehrspurig und unverbindlich statt. Das Kriterium für national zuständige Behörden wird aber teilweise erfüllt, da auf Bundesebene anhand des NCS Umsetzungsplans Verantwortlichkeiten für die Massnahmen festgelegt wurden.

2.3 Zusammenfassung

Abschliessend fasst die untenstehende Tabelle alle Massnahmen der NIS1-Richtlinie und deren Umsetzung in dem Schweizer Stromsektor zusammen. Weiter zeigt sie auch die Schnittstellen der Handlungsbereiche der NCS mit den Massnahmen der NIS-Richtlinie auf.

Es ist abermals hervorzuheben, dass der Quervergleich mit der NIS1-Richtlinie keinesfalls deren direkte Implementierung in der Schweiz vorschlägt. Der Vergleich zeigt primär, dass grundsätzlich die Stossrichtung der NCS mit jener der NIS-Richtlinie übereinstimmt. Dies bedeutet, dass die Massnahmen bereits grösstenteils deckungsgleich sind, wenn auch die Vorgaben der NIS1-Richtlinie bereits um einiges konkreter ausgearbeitet wurden. Die Schweiz ist zudem eng in das europäische Energiesystem eingebunden, was eine grosse gegenseitige Abhängigkeit auf die Sicherheit der Stromnetze hat. Die Vorgaben sollten daher zumindest angemessen Angeglichen werden.

Weiter gibt die NIS1-Richtlinie, wie in den Massnahmen deutlich wurde, lediglich ein Rahmenwerk für die Erarbeitung von nationalen Cyber-Vorgaben vor. Die Verpflichtungen sind zwar umfassend formuliert, können aber sehr verschieden interpretiert und schliesslich auch umgesetzt werden. Die Praxisbeispiele Deutschland und Frankreich in Anhang 5 verdeutlichen die sich abweichenden Implementierungen der NIS1-Richtlinie.

Tabelle 8: Quervergleich NIS1-Richtlinie und NCS 2018-2022 für identifizierte Handlungsfelder

EU NIS1 Verpflichtung			Mapping NCS 2018-2020	Umsetzungsstand Schweiz	Identifizierter Handlungsbedarf für den Schweizer Stromsektor
# 1	Nationale Strategie		**Verabschiedung der NCS 2018-2022**	✓	(Keiner)
# 2	EU-Kooperationsgruppe		Nicht direkt anwendbar, da kein EU-MS und daher nicht Mitglied der Gruppe.		
# 3	Netzwerk von Computer-Notfallteams		Nicht direkt anwendbar, da kein EU-MS, aber gewisse Relevanz für GovCERT.ch		
# 4	Sicherheitsanforderungen und Meldepflichten	Sicherheitsanforderungen	**NCS Massnahme 8:** Evaluierung und Einführung von Minimalstandards	⊗	Institutionalisierte *Rahmenbedingungen* betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor und damit verbunden, die Schaffung geeigneter und verhältnismässiger, technischer und organisatorischer Sicherheitsanforderungen für Cyber-Sicherheit und Resilienz innerhalb des Stromsektors Schweiz.
		Meldepflicht	**NCS Massnahme 9:** Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung	⊗	Das institutionalisierte *Meldewesen* betreffend laufende Cyber-Attacken innerhalb des Stromsektors Schweiz, inklusive der Einführung einer Meldepflicht.
		Überprüfung	**Impliziert duch NCS Massnahme 8**	⊗	Die institutionalisierte *Überprüfung* der getreuen Umsetzung bestehender Cyber-Regulierungen durch die Marktteilnehmer des Stromsektors Schweiz.
# 5	Ernennung von:	Nationale zuständige Behörden	**Allgemeine Bestimmungen der NCS und NCS Umsetzungsplan**	⇔	Die Festlegung von *Verantwortlichkeiten* (Institutionalisierung) für Cyber-Rahmenbedingungen, -Überprüfung, -Wissensaustausch und -Meldewesen im Stromsektor.
		Zentrale Anlaufstelle	**Schaffung NCSC im Rahmen der NCS**	✓	(Keiner)
		Nationales CERT	**NCS Massnahme 4:** Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage	⇔	Der institutionalisierte, laufende *Wissensaustausch* betreffend aktuelle Cyber-Gefahren (Threat Intelligence) innerhalb des Schweizer Stromsektors, sowie auf internationaler Ebene.

Abschliessend zeigt dieser Quervergleich auf, dass die Schweiz noch grossen und weiter zunehmenden Handlungsbedarf hat – insbesondere betreffend die NCS Massnahme 8 «Evaluierung und Einführung von Minimalstandards» und die NCS Massnahme 9 «Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung».

Wie die bisherige Diskussion in Kapitel 1 aufgezeigte, werden einige Schwachstellen bereits angegangen. Primär ist hier die Einführung der Meldepflicht bei KI hervorzuheben.[66] Zudem ist auch der Auftrag des Bundesrats an das NCSC und BWL in Zusammenarbeit mit den Fachämtern, die Einführung verpflichtende Sicherheitsstandards bis Ende 2022 zu prüfen, nennenswert.[67] Weiter besteht ein nationales CERT in der Schweiz, welches für den Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage, NCS Massnahme 4, zuständig ist. Jedoch sollte der bisherige sektorübergreifende Ansatz zum Wissensaustausch auf den Stromsektor konkretisiert werden, damit sich die Unternehmen gezielter auf die Cyber-Risiken vorbereiten können. Dies stellt ein zusätzlicher Aspekt dar, welcher in das Konzept einfliessen sollte.

Handlungsbedarf grundsätzlicherer Art, welcher noch nicht direkt angegangen wird, ist die Ernennung einer national zuständigen Behörde im Stromsektor bzw. ist das Verhältnis zwischen den bestehenden Behörden nicht geklärt. Dies wird bei der Entwicklung des Konzepts aufgegriffen.

Die restlichen Massnahmen der NCS, welche in Kapitel 1.1.1 NCS in Tabelle 1 als relevant für den Stromsektor hervorgehoben wurden, werden hier zwar nicht explizit erwähnt, sind aber als integrale Bestandteile der identifizierten Handlungsfelder zu verstehen. Beispielsweise wird Massnahme 11 «Aufbau von Expertise zu Fragen der Standardisierung in Bezug auf Cyber-Sicherheit» in allen Handlungsfeldern implizit angenommen, da diese gewissermassen für die Umsetzung vorausgesetzt werden muss.

Es soll an dieser Stelle festgehalten werden, dass sich die Schere zwischen EU Staaten und der Schweiz bezüglich Cyber-Sicherheit im Stromsystem weiter und weiter öffnet. Während in der Schweiz noch grundsätzliche Fragen der NIS1 angegangen werden müssen so wird bereits mit Hochdruck an der Weiterentwicklung und Implementierung der NIS2 in den EU Staaten gearbeitet. Der Network Code Cyber Security, welcher in kürzerer Frist aktiv sein dürfte, dürfte zudem den Rückstand im Stromsektor zusehends vergrössern, zwar ist Swissgrid Mitglied der ENTSO-E aber die die Akteure des Schweizer Stromsektors sind nicht zwingend angehalten, die Network Codes der EU zu implementieren.

---

66 Bundesrat (2020), Medienmitteilung: Bundesrat spricht sich für eine Meldepflicht für kritische Infrastrukturen bei Cyberangriffen aus.

67 Bundesrat (2018a), Medienmitteilung: Bundesrat nimmt Schlussbericht der Expertengruppe «Zukunft der Datenbearbeitung und Datensicherheit» zur Kenntnis.

Fazit Kapitel 2 Quervergleich des regulatorischen Umfelds der EU und der Schweiz

Dieser Quervergleich mit der EU bedeutet nicht, dass der Schweizer Strommarkt die NIS1-Richtlinie unverändert übernommen sollte. Aufgrund der starken Vernetzung der Märkte und den damit verbundenen gegenseitigen Abhängigkeiten, ist aber ein angemessenes Angleichen an die umliegenden regulatorischen Vorgaben sehr empfehlenswert. Der Exkurs betreffend Einordnung der regulatorischen Entwicklungen in den Vereinigten Staaten zeigt, dass die Anforderungen der NIS1 im Vergleich sogar eher moderat erscheinen und ein Angleichen an das amerikanische, sehr detaillierte Cyber-Sicherheit Regulierungssystem im Stromsektor für die Schweiz nicht umsetzbar ist. Die NCS 2018-2022 hat einige der Ziele und Massnahmen der NIS1-Richtlinie für die Schweiz übernommen und wo sinnvoll adaptiert.

Allerdings besteht für eine erfolgreiche Umsetzung der NCS 2018-2022 im Stromsektor noch erheblicher Handlungsbedarf insbesondere in regulatorischer Hinsicht. Grundsätzlich ergeben sich aus vier Handlungsfelder betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor: Rahmenbedingungen, Überprüfung, Meldewesen und Wissensaustausch. Zusätzlich müssen grundlegende Fragen geklärt werden. Darunter fällt die Festlegung von Verantwortlichkeiten der national zuständigen Behörde(n) diese Handlungsfelder, weshalb diese Massnahme eine Voraussetzung ist für die anderen vier und daher bei der Erarbeitung des Zielzustands in allen Bereichen implizit berücksichtigt werden muss.

Besonders bedenklich ist die hohe Dynamik der internationalen Entwicklungen zur Cyber-Sicherheit, insbesondere hinsichtlich des Stromsektors. Mit der mit Hochdruck vorangetriebenen Weiterentwicklung der NIS2 Richtlinie öffnet sich die sowieso schon grosse Schere in Bezug auf die Cyber-Sicherheit im Stromsektor zwischen internationalen und Schweizer KI Betreibern zusehends. Die Erarbeitung und in näherer Zukunft vorgesehene Implementierung des «Cybersecurity Network Code» beschleunigt diese Entwicklung noch zusätzlich. Dieses zügige Voranschreiten ist gänzlich eine andere als die Dynamik, welche die Schweizer Regulierung des Stromsektors derzeit aufweist, was mit Blick auf die Versorgungssicherheit sogfältig beobachtet und Massnahmen zeitnah geprüft werden sollten.

Die bisherigen Darstellungen lassen einen grossen Handlungsbedarf im Stromsektor vermuten. Da aber wie in Kapitel 1.2.1 Allgemeine Zuständigkeiten im Stromsektor das Subsidiaritätsprinzip[68] ein zentrales Element der Stromversorgung ist, wird im nächsten Kapitel zunächst geklärt ob und in welchen Cyber-Sicherheitsbereichen ein staatliches Eingreifen tatsächlich nötig ist. Daten und Informationen hierzu sind bis anhin nur sehr beschränkt verfügbar, weshalb eine nationale E-Survey im Rahmen dieses Berichts durchgeführt wurde. Somit sollte erstmals ein ausführliches und gesamtheitliches Bild zu der aktuellen Lage gezeichnet werden, um darauf basierend notwendige Aktivitäten ableiten zu können.

[68] Dies bedeutet ein grundsätzlicher Vorrang privater Massnahmen vor staatlichen Massnahmen.

3 Resultate der nationalen E-Survey 2020

Die bisherigen Kapitel fokussierten sich auf das regulatorische Umfeld betreffend Cyber-Sicherheit und Resilienz im Stromsektor. Tabelle 8 verdeutlichte, dass grosser regulatorischer Handlungsbedarf im Stromsektor besteht, damit die NCS 2018-2022 im vorgegebenen Zeitrahmen erreicht werden kann.

In diesem Kapitel wird zum ersten Mal ein möglichst gesamtheitliches Bild zu der momentanen technischen Lage anhand einer eigenen Erhebung gezeichnet, damit ermittelt werden kann, ob und in welchen IT/OT-Bereichen bei den Unternehmen der Elektrizitätswirtschaft tatsächlich praktische Mangellagen bestehen. Diese Erkenntnisse sind essentiell, um dem Subsidiaritätsprinzip[69] entsprechend ein Zielbild und Massnahmen abgeleitet werden können. Denn falls die Unternehmen in der Absenz von staatlichen Eingriffen bereits über angemessene Fähigkeiten betreffend Cyber-Sicherheit und Resilienz verfügen, wären Massnahmen gegebenenfalls nicht zwingend nötig.

Da es bezüglich dem Stand der Cyber-Sicherheit keine oder nur sehr wenige Daten zum Strommarkt gibt, mussten diese zunächst ermittelt werden.[70] So wurde eine Umfrage (E-Survey) erstellt und digitalisiert per Website durchgeführt. Der Fragebogen orientierte sich eng an dem seit 2018 den Unternehmen der Elektrizitätswirtschaft bekannten IKT Minimalstandard (vgl. Kapitel 1.2.2 Besehende Vorhaben). Des Weiteren, wurde der Fragebogen mit Blick auf die Einführung von Smart Metern und anderen aktuellen Entwicklungen (z.B. Cloud) ergänzt. Die Antwortmöglichkeiten der Teilnehmer auf die jeweiligen Fragen wurden vordefiniert und mittels Auswahlmenü zur Verfügung gestellt, um den Aufwand möglichst gering zu halten. Ein Bemerkungsfeld ermöglichte den Markteilnehmern zusätzliche Kommentare einzufügen.

Die Erhebung war freiwillig und Erhebung wurde zwischen April 2020 bis Juli 2020 online durchgeführt. Es zeigte sich, dass eine grosse Herausforderung dahingehend bestand, eine Übersicht der im Strommarkt tätigen Unternehmen zu bekommen, um zu evaluieren, welche Unternehmen zu kontaktieren sind. So existiert z.B. kein Überblick über die im Markt tätigen Messdienstleistungsunternehmen. Mit grossen Aufwand konnte eine gewisse Teilmenge aller im Strommarkt tätigen Unternehmen identifiziert werden. Eine weitere Herausforderung stellt sodann die Frage der zu verwendeten Kontaktdaten. Aufgrund der hohen Bedeutung für die vorliegende Analyse wurde die Befragung mit mehreren Aufrufen zur Teilnahme durch das BFE und Branchenverbände wie dem VSE oder dem Schweizer Wasserverband (SWV) flankiert. Die Befragung war auf 30 Minuten ausgelegt, jedoch wurde teilweise angegeben, dass die Teilnehmenden bis zu zwei Stunden benötigten. Gründe hierfür waren sehr heterogen. So war es offenbar schwierig Zuständige zu identifizieren, und/oder Begrifflichkeiten in den Fragen zu entsprechen, da sie nicht bekannt waren und zunächst recherchiert werden mussten. Generelle Rückmeldungen bemängelten die äusserst hohe Komplexität der Fragen im Allgemeinen.

Die Maturität in den gemäss IKT Minimalstandard vorgegeben Bereichen wurde von den Unternehmen selbst eingeschätzt und es wurden keine Nachweise gefordert. Es ist davon auszugehen, dass diese Selbsteinschätzungen teils zu optimistisch eingestuft wurden, da z.B. die relevanten Fachkenntnisse für eine objektivere Bewertung beschränkt waren. Umgekehrt kann die Selbsteinschätzung aber auch zu negativeren Maturitätseinstufungen geführt haben, um z.B. gewisse zukünftige Investitionen in den Be-

---

[69] Wie in Kapitel 1.2.1 Allgemeine Zuständigkeiten im Stromsektor vorgestellt, impliziert das Subsidiaritätsprinzip ein grundsätzlicher Vorrang privater Massnahmen vor staatlichen Massnahmen.

[70] Zwei wesentliche Anhaltspunkte sind hierbei das Quick Assessment der Electrosuisse (2019) «Cybersecurity bei kleinen und mittleren Elektrizitätsversorgungsunternehmen» und der Bericht der ElCom (2019) «Cyber-Sicherheit». Die Argumentation in diesem Bericht wurde teils durch die Erkenntnisse der beiden Dokumente ergänzt.

reich zu begründen. Kurzum, trotz dem standardisierten Fragebogen, war eine objektive Bestandsaufnahme durch die subjektiven Selbsteinschätzungen ohne Nachweisforderung beeinträchtigt. Dennoch kann angenommen werden, dass die relative Verteilung der Realität in Annäherung entspricht.

Die Auswertung der Umfrage erfolgt entlang der folgenden **vier Analysebereichen**:

1. Aussagekräftigkeit der Umfrage

   Welche Unternehmen haben an der Erhebung teilgenommen? Wie ist die generelle Verteilung innerhalb der Teilnehmer und wie repräsentativ ist die E-Survey im Vergleich zum Gesamtmarkt Schweiz?

2. Aktuelles Maturitätsniveau der IT-Sicherheit im Stromsektor Schweiz

   Wie stehen alle Umfrage-Teilnehmer betreffend Ihrer Maturität im Bereich der IT Sicherheit basierend auf den eigenen Angaben?

3. Aktuelles Maturitätsniveau der OT-Sicherheit im Stromsektor Schweiz

   Wie stehen alle Umfrage-Teilnehmer betreffend Ihrer Maturität im Bereich der IT Sicherheit basierend auf den eigenen Angaben?

4. Weitere Erkenntnisse und Auffälligkeiten

   Welche weiterführenden Erkenntnisse konnten aus der Umfrage gezogen werden?

Diese Einteilung bedeutet, dass zuerst in den Analysenbereichen 1-3, generelle Beobachtungen und Schlussfolgerungen entlang der konkreten Fragen in der Umfrage aufgeführt werden. Erst danach, in Analysenbereich 4, werden die verschiedenen Erkenntnisse korreliert[71] und weiterfassende Einsichten erklärt.

In den nachfolgenden Unterkapiteln werden die Haupterkenntnisse der nationalen E-Survey hervorgehoben und entlang der vier Analysenbereiche ausgewertet. In Anhang 1 werden die Resultate ausführlich dargestellt und genauer erläutert.

[71] Korrelationen beschreiben eine Beziehung zwischen zwei oder mehreren Merkmalen, Zuständen oder Funktionen. Die Beziehung muss keine kausale Beziehung sein, d.h. manche Elemente eines Systems beeinflussen oder begründen sich gegenseitig nicht.

3.1 Aussagekraft der Umfrage

Insgesamt haben 124 Teilnehmer an der E-Survey 2020 teilgenommen. Der Fokus der Umfrage richtete sich bei allen Unternehmen gezielt auf die eigenen Tätigkeiten im Zusammenhang mit dem Stromsektor. Es nahmen teil[72]:

- 113 Netzbetreiber. Dies entspricht, gemäss Angaben der ElCom, rund 18% der Gesamtmenge aller existierenden Netzbetreiber des Gesamtmarktes Schweiz im Jahr 2019.
- 54 Produzenten. Etwa 50% aller Stromproduzenten, welche durch das BFE für die Umfrage angefragt wurden.
- 79 Messstellenbetreiber. Gemeinsam decken sie ungefähr 40% aller existierenden Messpunkte in der Schweiz im Jahr 2019 ab.

Zur Beantwortung der Umfrage wurden die folgenden Bereiche bewusst ausgeklammert:

- Nuklearreaktoren: Diese sind bereits spezifisch reguliert, auch im Bereich der Cyber-Sicherheit, durch das Eidgenössische Nuklearsicherheitsinspektorat (ENSI), dennoch wurden die Betreiberfirmen befragt, da sie weitere Kraftwerke besitzen und betreiben;
- Energiehandelstätigkeiten: der Fokus wurde auf inländische Betriebe gesetzt. Weiter gab es keine vollständige Übersicht der Händler und ihre Bedeutung im Bereich der Cyber-Sicherheit erschien untergeordnet; und
- Weiterführende Energiedienstleistungen, welche in die Messung und Steuerung elektrischer Anlagen involviert sind (bspw. Smart-Home Applikationen, Aggregatoren mit IoT-Anwendungen, wie z.B. Wärmepumpen- oder Elektromobilsteuerungen). Da in erster Näherung ein Überblick über die Marktstruktur nicht vorhanden war, mussten solche Unternehmen aus der Befragung ausgeschlossen werden.

Die Teilnehmer mussten zunächst jeweils angeben, ob sie unternehmerisch als Netzbetreiber, als Produzent und/oder als Messstellenbetreiber agieren. Zusätzlich wurde gefragt, ob die Teilnehmer rein nur im Strommarkt tätig sind oder auch mit anderen Energieträgern agieren (z.B. als Gasnetzbetreiber). Daraus ergaben sich die folgenden elf Kombinationsmöglichkeiten für die Kategorisierung der Unternehmenstypen:

- Netzbetreiber;
- Produzent (nur Strom);
- Produzent (Strom und anderes);
- Messstellenbetreiber (nur Strom);
- Messstellenbetreiber (Strom und anderes);
- Netzbetreiber und Produzent (nur Strom);
- Netzbetreiber und Produzent (Strom und anderes);
- Netzbetreiber und Messstellenbetreiber (nur Strom);
- Netzbetreiber und Messstellenbetreiber (Strom und anderes);
- Netzbetreiber, Produzent und Messstellenbetreiber (nur Strom); oder
- Netzbetreiber, Produzent und Messstellenbetreiber (Strom und anderes).

[72] Wie nachfolgend erklärt sind, wurden gewisse Unternehmen entlang der Unternehmenstypen mehrfach gezählt, weshalb die Anzahl Teilnehmer in der Aufzählung die total angegebenen Teilnehmer (= 124) übersteigt.

Aus Abbildung 8 ergibt sich, dass jeweils fast ein Drittel der Teilnehmer sich entweder als «Netzbetreiber» oder als «Netzbetreiber, Produzent und Messstellenbetreiber (Strom und anderes)» identifiziert haben.

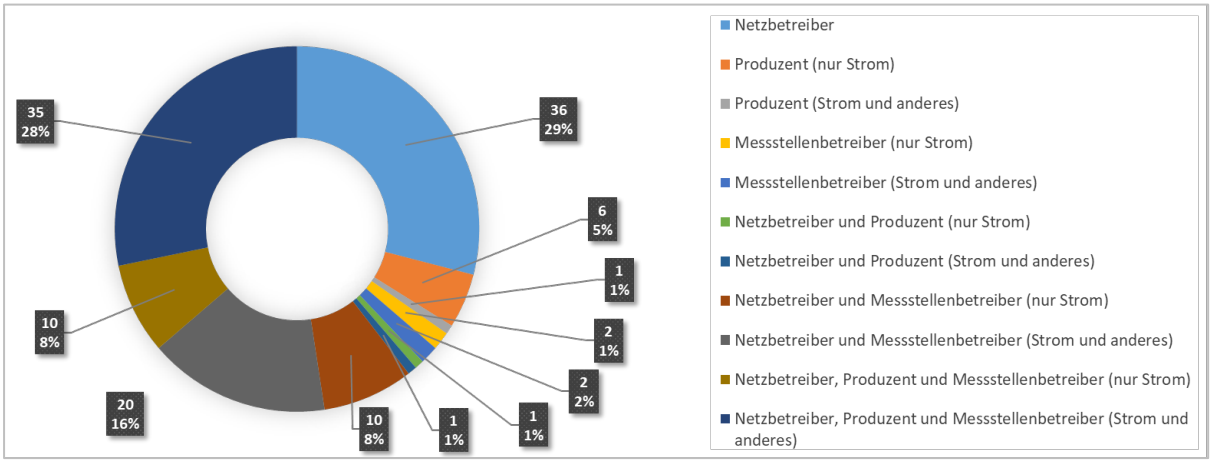


Abbildung 8: E-Survey Teilnahme – nach Unternehmenstyp

Zu beachten - Diese elf Unternehmenstypen wurden aus Komplexitätsgründen bei den Auswertungen für die IT- oder OT-Maturität in den Analysebereichen fünf übergeordneten Kategorien zugeteilt:

1) Netzbetreiber;
2) Produzent – nur Strom;
3) Produzent – Strom und anderes;
4) Messstellenbetreiber – nur Strom; und
5) Messstellenbetreiber – Strom und anderes.

Dies bedeutet, dass bei den nachfolgenden Auswertungen bezüglich der IT- oder OT-Maturität Unternehmen, welche mehreren Unternehmenstypen gleichzeitig angehören, jeweils in jede der einzelnen Kategorien für die jeweilige Berechnung der Durchschnittswerte miteinbezogen wurden. Ein Unternehmen, welches als Produzent (nur Strom) und Netzbetreiber agiert, ist in den nachfolgenden Analysen als «Produzent – nur Strom» und «Netzbetreiber» vertreten. Teils können Unternehmen gar in drei Kategorien als Netzbetreiber, Produzent (Strom und/oder anderes), sowie Messstellenbetreiber (Strom und/oder anderes) gezählt sein. Dies beeinträchtigt die Aussagekräftigkeit der Umfrage nicht, da stets Durchschnittswerte pro Kategorie ausgewertet wurden und Quervergleiche zwischen den Kategorien vermieden wurden.

In der E-Survey wurden weiterführende Fragen zu der Positionierung der Unternehmen im Stromsektor erhoben, deren Auswertung in Anhang 1 zu finden sind.

Zusammenfassend kann festgehalten werden, dass mit 124 Unternehmen unterschiedlicher Grössen eine genügend repräsentative Menge des Energiesektors der Schweiz an der Umfrage teilgenommen hat, um aussagen treffen zu können. Gleichzeitig ist es jedoch bemerkenswert, dass trotz hoher Relevanz des Themas Cyber-Sicherheit in der Branche, doch wiederrum nur ein so kleiner Anteil teilgenommen hat. Die Teilnehmer lassen sich anhand ihrer Unternehmenstypen wie folgt kategorisieren:

- Die vertretenen 113 Netzbetreiber erreichten 68% der jährlichen Gesamtstromeinspeisung in der Schweiz im Jahr 2019, ohne Berücksichtigung der Nuklearenergie;
- Die 54 Produzenten erzielten 43% der Stromproduktion der Schweiz im Jahr 2019, ohne Berücksichtigung der Nuklearenergie.
- Die 79 Messstellenbetreiber decken etwa 40% aller existierenden Messpunkte in der Schweiz im Jahr 2019 ab.

Zahlreiche kleinere bis mittlere Betriebe haben ebenfalls an der Umfrage teilgenommen, sind aber im Vergleich zu den grösseren Unternehmen anzahlmässig weniger stark repräsentiert. Dies sollte aber die Aussagekraft der Auswertung nicht beeinflussen, da die Grösse der Betriebe nicht direkt mit deren Maturitätsniveau gleichgesetzt wurde und die Durchschnittswerte per Unternehmenstyp belastbarer für Aussagen zur Cyber-Sicherheit und -Resilienz sind.

3.2 Aktuelles Maturitätsniveau der IT- / OT-Sicherheit

Nachdem im ersten Analysebereich primär die Aussagekraft und Repräsentativität der Umfrage analysiert wurde, fokussiert sich dieses Unterkapitel auf die gemachten Selbsteinschätzungen betreffend Maturität der Teilnehmer in den Analysebereichen zur IT- und OT.

Diese beiden Module werden in dem gleichen Kapitel besprochen, da beide Teile auf dem gleichen Fragebogenteil aufbauen. Wie in Kapitel 1.2.2 Bestehende Vorgaben dargelegt wurde, wurde der IKT Minimalstandard vom Bundesamt für wirtschaftliche Landesversorgung (BWL) im Jahr 2018 veröffentlicht und dient als Empfehlung und mögliche Richtschnur zur Verbesserung der allgemeinen IKT-Resilienz. Er richtet sich primär an die Betreiber von kritischen Betrieben, ist aber grundsätzlich für jedes Unternehmen anwendbar. Das Handbuch «Grundschutz für Operational Technology (OT)» des Branchenverbands VSE wurde, wo relevant, als weiterführende Richtlinie angegeben.

Der Fragebogen folgt dem IKT Minimalstandard in dem Aufbau der Fragen und besteht aus fünf Funktionen:

- Identifizieren («Identify»): befasst sich mit der Entwicklung für das organisatorische Verständnis des eigenen Unternehmens.
- Schützen («Protect»): unterstützt die Fähigkeit zur Verhinderung von Cyber-Sicherheitsvorfällen.
- Erkennen («Detect»): diese Funktion bietet einen relativ neuen Blickwinkel auf die Informationssicherheit und ergänzt die traditionellen Sicherheitsziele auf die Identifikation eines möglichen Vorfalls. Erfahrungen haben gezeigt, dass Unternehmen heutzutage davon ausgehen müssen bereits Ziel eines – meist erfolgreichen – Angriffs geworden zu sein oder in der Zukunft zu werden und deshalb wird diese Funktion zunehmend wichtiger.
- Reagieren («Respond»): wird eine Cyberattacke einmal erkannt zielt diese Funktion darauf ab, diese möglichst schnell und effizient bekämpfen zu können.
- Wiederherstellen («Recover»): nach einer Attacke müssen betroffene Systeme wiederhergestellt werden sowie kontinuierliche Verbesserungsprozesse dürfen nicht vernachlässigt werden.

Wie bereits dargelegt, wurden die Umfrageteilnehmer gefragt, gemäss 'IKT Minimalstandard' die eigene Maturität pro Unterkategorie in eine von fünf Maturitätsstufen ('Levels') selbst einzuschätzen.[73]

- Maturitätsstufe 0: Nicht Umgesetzt.
- Maturitätsstufe 1: Partiell umgesetzt, nicht vollständig definiert und abgenommen.
- Maturitätsstufe 2: Partiell umgesetzt, vollständig definiert und abgenommen.
- Maturitätsstufe 3: Umgesetzt, vollständig oder grösstenteils umgesetzt, statisch.
- Maturitätsstufe 4: Dynamisch, umgesetzt, kontinuierlich überprüft, verbessert.

In Anhang 1 werden die fünf Funktionen des IKT Minimalstandards, sowie konkreten Kriterien für die Maturitätsstufen erläutert.

[73] Die unabhängige Electrosuisse Umfrage verwendete die gleiche Struktur sowie Maturitätsstufen entlang des IKT Minimalstandards, aber war begrenzt auf die Befragung von kleinen und mittleren Elektrizitätsversorgungsunternehmen bzw. den Produzenten.

Schliesslich ergibt sich im Bereich der IT-Sicherheit das folgende Bild über alle 124 Umfrageteilnehmer entlang der fünf IKT Minimalstandard Funktionen:

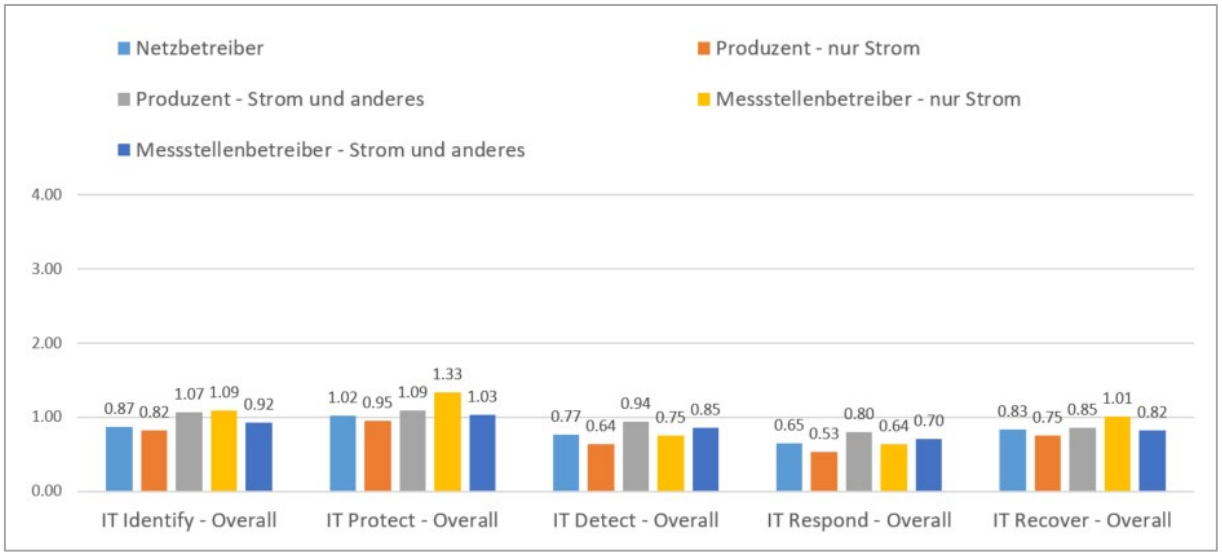


Abbildung 9: Maturität IT-Sicherheit

Der generelle Stand der Maturität ist sehr niedrig. Kaum eine Cyber-Fähigkeit erreicht einen Wert über der Maturitätsstufe 1, welche als rudimentäre Basisstufe gilt. Die Cyber-Risiken, werden so gemäss Auslegung, oftmals nur ad-hoc oder reaktiv verwaltet. Auch scheinen Risikomanagementprozesse und organisatorische Vorgaben zur IKT-Sicherheit des Öfteren als nicht formalisiert. Es ist davon auszugehen, dass aufgrund der fehlenden Prozessen keine abschliessende Sicht über die Sicherheitsrisiken innerhalb der IT-Landschaft gegeben ist.

Es ist weiter auffällig, dass die aktuelle Maturität in den Bereichen «Identifizieren» und «Schützen» etwas höher ist, als die Fähigkeiten bei der «Erkennung» und der «Reaktion» auf Cyber-Vorfälle, sowie bei der «Erholung» nach einem Vorfall. Dies kann so gedeutet werden, dass der Fokus in der Vergangenheit bisher stärker auf präventive Massnahmen gesetzt wurde und reaktive Fähigkeiten tendenziell im Verhältnis vernachlässigt wurden. Es fehlt demnach an Reaktionsplänen im Ereignisfall und die Cyber-Risiken werden kaum vollumfänglich adressiert. Vordefinierte Prozesse, Strategien und Verantwortlichkeitsbereiche würden helfen, die weitere Ausbreitung eines Cyber-Sicherheitsvorfalls zu verhindern und den möglichen Schaden zu begrenzen.

Wie in der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022 festgehalten wurde, zeigt sich zunehmend, dass Unternehmen heutzutage entweder bereits Ziel eines – meist erfolgreichen – Angriffs geworden sind oder davon ausgehen müssen, es in naher Zukunft zu werden. Ein genereller Paradigmenwechsel von Cyber-Sicherheitsexperten geht davon aus, dass für präventive Cyber-Massnahmen gesorgt sein muss, aber dass diese nicht mehr vollständig vor einen Cyber-Sicherheitsvorfall schützen können.[74] Durch die Kompetenzsteigerung der Angreifer, sowie technologische Entwicklungen, wird die Verminderung allfälliger Schäden immer zentraler und der Fokus von der Verteidigung gegen externe Gefahren auf interne Verteidigungsstrukturen erweitert. Die Cyber-Resilienz und die IKT Fähigkeiten «Erkennung», «Reaktion» und «Erholung» gewinnen dadurch immer mehr und schneller an Bedeutung.

[74] European Union Agency for Cybersecurity (2020), ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.

Im Bereich der OT-Sicherheit zeigt sich ein ähnliches Bild der Maturitätswerte über alle 124 Umfrageteilnehmer entlang der fünf IKT Minimalstandard Funktionen:

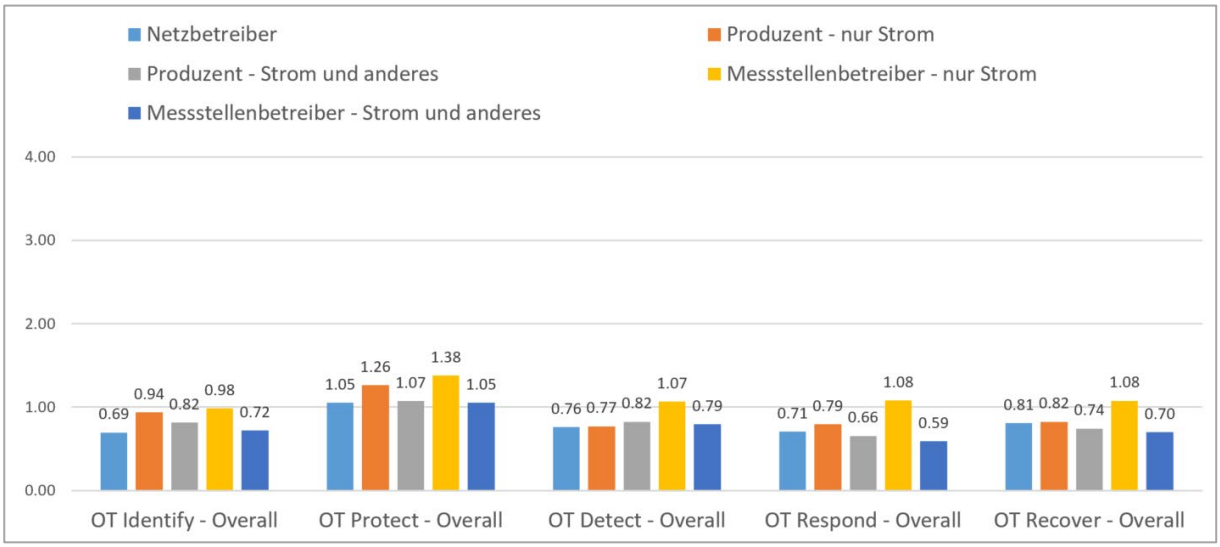


Abbildung 10: Maturität OT-Sicherheit

Kaum eine Cyber-Fähigkeit erreicht die grundlegende Maturitätsstufe 1. Grundsätzlich glauben die Teilnehmer ihre OT-Landschaft etwas besser gehärtet zu haben als ihre IT (vgl. «Schützen» Kategorie von Analysebereich 2 in Abbildung 9 Werte zwischen 0.95 und 1.33; mit Analysebereich 3 Abbildung 10 Werte zwischen 1.05 und 1.38).

Bei der detaillierten Auswertung der OT-Kategorien zeigt sich weiter, dass den Unternehmen die Risiken innerhalb der OT-Landschaft tendenziell nicht bekannt sind. Bis anhin wurde offenbar in der Regel versucht, als Sicherheitsstrategie OT-Netzwerke und Systeme physisch abzugrenzen. Die Identifikation von Sicherheits-Risiken beschränkte sich daher primär auf physische Sicherheitsparameter (z.B. 24/7 Überwachung der Anlagen, physischer Zugang) und der Fokus lag auf der ständigen Verfügbarkeit der Systeme.

Die OT-Kategorie «Schützen» erreicht vergleichsweise eine höhere Maturitätsstufe, wenn auch nur knapp über der Stufe 1. Dieses Bild ist wohl so zu begründen, dass OT-Landschaften in der Energie in der Regel in einer abgeschotteten Infrastruktur betrieben werden und es sich bei den Systemen (SCADAs, etc.) meist um bereits gehärtete Standardlösungen von Drittanbietern handelt.

Schliesslich war erkennbar, dass OT-Risiken noch nicht anhand von formalisierten Prozessen und organisatorischen verwaltet werden.

Zusammenfassend ergibt sich das folgende Bild im Durchschnitt über beide Bereiche.

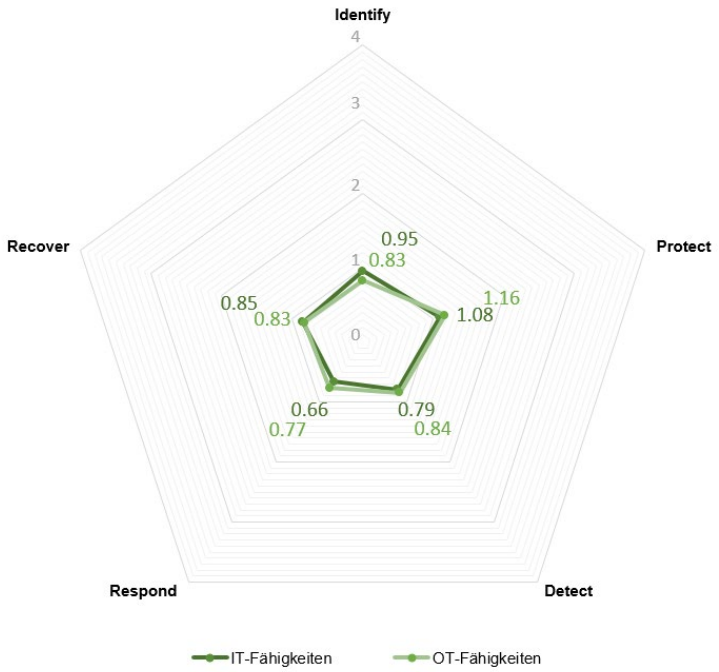


Abbildung 11: Durchschn. IKT Maturitätsstand des Schweizer Stromsektors – «E-Survey» Resultate 2020

Abschliessend führten Analysebereiche 2 (IT) und 3 (OT) zu den folgenden Erkenntnissen:

- Im Schnitt ist die Maturität der befragten Unternehmen in beiden Bereichen der IT- und OT-Sicherheit sehr niedrig.
- Die Betriebe sind demnach der eigenen Branchenrichtlinie nicht nachgekommen und sind noch weit entfernt von dem eigenen gesetzten Ziel einer 2.6 als Maturitätsstufe.
- Sowohl in der IT- und OT-Sicherheit werden Cyber-Bedrohungen bei dem Grossteil der Unternehmen noch nicht mit den nötigen Massnahmen vermindert.
- Bei der Funktion «Schützen» ist die Maturität der OT-Sicherheit leicht höher jene der IT-Sicherheit, was darauf basieren kann, dass OT-Systeme anscheinend bisher physisch abgeschottet wurden und die Unternehmen grundsätzlich der Sicherheit der OT-Hersteller vertrauen.
- Die Funktionen «Erkennen» und «Reagieren» verzeichnen in der IT-Sicherheit die tiefsten Maturitätswerte. Der Fokus der Unternehmen muss daher dringend verstärkt auf reaktive Fähigkeiten gesetzt werden.

Anhang 1 vertieft die Auswertung der Maturität entlang der fünf Funktionen und bietet eine weitergehende Analyse.

3.3 Weitere Erkenntnisse und Auffälligkeiten

In diesem letzten Teil der Umfrageauswertung werden Korrelationen und Auffälligkeiten diskutiert, um weitere Erkenntnisse gewinnen zu können.

Basierend auf der Analyse von Analysebereich 4 in Anhang 1 wurden die folgenden zentralen Erkenntnisse aus der E-Survey gezogen:

- Das Vorhandensein einer IT-/OT-Strategie korreliert stark positiv mit der Maturität im IT-/OT-Sicherheitsbereich. Rund 50% der Teilnehmer verfügen über eine explizite IT-/OT-Strategie und erreichen Werte klar über der Maturitätsstufe 1. Jene Unternehmen, welche angeben, dass diese Strategie in Bearbeitung sei, weisen eine deutlich höhere Maturität (zwischen Maturitätsstufe 0 und 1) auf als jene die die Frage verneinten (nah an Maturitätsstufe 0).
- Die generell höchsten Maturitätswerte erzielten Unternehmen, welche die OT-Sicherheit über die IT-Sicherheit priorisieren. Hier besteht die Annahme, dass jene Betriebe mit einer gewissen Grundmaturität im IT-Bereich, ihren Fokus vermehrt auf die OT-Sicherheit verschieben, um ihre Kompetenzen im OT-Bereich auf ein ähnliches Niveau zu steigern.
- Es lassen sich keine eindeutigen Korrelationen betreffend angegebenes Maturitätsniveau und Anzahl dedizierte Mitarbeiter für IT-/OT-Sicherheit erkennen. Diese Aussage ist aber zu relativiert werden, da viele Mitarbeiter insbesondere für OT mehrere Funktionen innerhalb ihres Betriebes wahrnehmen und nicht ausschliesslich für Sicherheit zuständig sind.
- Für Unternehmen bei welchen die Gesamtverantwortung für Cyber-Sicherheit beim Leiter IT liegen fielen die angegebenen Maturitätswerte im Schnitt höher aus (IT-Sicherheit = 1.09; OT-Sicherheit = 0.9). Umgekehrt haben Unternehmen, bei welcher die Gesamtverantwortung dem Leiter Produktion (= näher an OT) zugeteilt ist, im Schnitt eher tiefere Werte. Auch fielen Werte deutlich höher aus, wenn das obere Kader die Gesamtverantwortung trägt (IT-Sicherheit = 1.26; OT-Sicherheit = 1.49). So lässt sich wohl schliessen, dass wenn Cyber-Risiken als Chefsache wahrgenommen werden, mehr Aufwand zu deren Verminderung betrieben wird.
- Die Maturitätswerte bei jenen Unternehmen, welche die Verantwortlichkeit für Cyber-Sicherheit nicht klar definiert haben, fallen wenig überraschend sehr tief aus (IT-Sicherheit = 0.37; OT-Sicherheit = 0.41).
- Eine grosse Mehrheit der Umfrageteilnehmer (69%) befürwortet eine Meldepflicht von Cyber-Sicherheitsvorfällen. 26 Teilnehmer der E-Survey sind Mitglieder des geschlossenen Kundenkreises von MELANI und weisen im Schnitt ein merkbar höheres Maturitätsniveau aus (IT-Sicherheit = 1.11; OT-Sicherheit = 1.11). Nicht MELANI Mitglieder hingegen erreichen tiefer Maturitätsstufen (IT-Sicherheit = 0.76; OT-Sicherheit = 0.76).
- Die Mehrheit aller Umfrageteilnehmer (83%) bestätigte, dass Cyber-Sicherheitsaspekte bei der Einführung neuer Smart Meter in die bestehende Unternehmensarchitektur mitberücksichtigt werde und es liess sich eine positive Korrelation mit dem Reifegrad dieser Teilnehmer betreffend ihrer IT- / OT-Sicherheit feststellen.

Diese Beobachtungen werden bei der Entwicklung für mögliche Verbesserungsansätze zur Cyber-Sicherheit und Resilienz für den Schweizer Strommarkt richtungweisend sein.

3.4 Zusammenfassung

Fazit Kapitel 3 Aktueller Stand - Resultate der nationalen E-Survey 2020 betreffend Cyber Security und Resilienz im Stromsektor

Die Auswertung der E-Survey bezüglich der IT-/OT-Sicherheit-Maturität der Schweizer Strommarktteilnehmer zeigt deutlich, dass die Akteure noch nicht die notwendigen IT-/OT-Massnahmen getroffen haben, um den steigenden Cyber-Risiken entgegenzuwirken. Obwohl Cyber-Sicherheit als eine Priorität der Unternehmen der Schweizerischen Elektrizitätswirtschaft zur weiteren Gewährleistung einer hohen Versorgungssicherheit postuliert wurde, haben deutliche weniger als die Hälfte der angefragten Unternehmen an der E-Survey teilgenommen. Bei den Netzbetreibern waren es gar lediglich nur rund 18% der Gesamtmenge aller existierenden Netzbetreiber des Gesamtmarktes Schweiz im Jahr 2019.

Das allgemeine Maturitätsniveau der Schweizer Stromversorger ist im Schnitt tief. Kaum eine Cyber-Fähigkeit erreicht einen Wert über der Maturitätsstufe 1, welche als rudimentäre Basisstufe gilt. Cyber-Risiken werden offenbar ad-hoc oder reaktiv verwaltet. Risikomanagementprozesse und organisatorische Vorgaben zur IKT-Sicherheit scheinen nicht formalisiert. Die Betriebe sind demnach der eigenen Branchenrichtlinie nicht nachgekommen und sind noch weit entfernt von dem eigenen gesetzten Ziel einer 2.6 als Maturitätsstufe. Die Verantwortlichkeiten und Prozesse für Cyber-Sicherheit und Resilienz ist bei vielen Unternehmen nicht institutionalisiert. Die Cyber-Sicherheit wird oft als Nebentätigkeit mit geringer Priorität angesehen. Jedoch ist auch anzumerken, dass die Unternehmen auch über eine gewisse Grösse verfügen müssen, um überhaupt die Möglichkeit für die Einsetzung eines CISO und/oder IT-/OT-Leiter zu haben. Teilweise konnten die Fragen zum seit 2018 etablierten IKT Minimalstandard nicht oder nur mit viel Aufwand beantwortet werden. Offenbar wird seitens der Akteure in der Mehrzahl klare Massnahmen begrüsst, wie etwa die Etablierung einer Meldepflicht.

Der in Kapiteln 1 und 2 vermutete Handlungsbedarf scheint sich durch die Befragung zu erhärten bzw. die Möglichkeit, dass die Stromversorger im Sinne der Subsidiarität ausreichende Massnahmen vorgesehen haben nicht zu bestätigen. Dies unterstreicht die regulatorischen Handlungsbedürfnisse für den Schweizer Stromsektor betreffend Cyber-Sicherheit und Resilienz, denn die privaten Massnahmen haben gemäss Resultat der nationalen E-Survey noch nicht zu der nötigen Stärkung der betrieblichen Cyber-Fähigkeiten geführt.

4 Vorgeschlagene Optionen zur Adressierung des Handlungsbedarfs

In den vorhergehenden Kapiteln wurde der aktuelle Stand betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor erarbeitet. Es wurde ein Vergleich mit der NIS-Richtlinie gezogen, welche in Europa bezüglich Cyber-sicherheit massgebend ist, und entlang der aktuellen NCS-Strategie der Schweiz evaluiert. Damit konnte identifiziert werden in welchen Bereichen im Stromsektor Schweiz aktuell Handlungsbedarf betreffend Cyber-Sicherheit und Resilienz bestehen könnte. Die E-Survey bestätigte, dass das zeitnahe Erreichen eines den Gefahren angepassten Zielzustandes ohne staatliche Eingriffe kaum realistisch ist.

Gemäss der Zusammenfassung in Kapitel 2 sind diese vier Handlungsfelder gemäss der Kategorisierung in Tabelle 8 für den Zielzustand bzgl. Cyber-Sicherheit und Resilienz im Stromsektor relevant:

Kapitel 4.1 – Rahmenbedingungen

Die Schaffung von Rahmenbedingungen im Schweizer Stromsektor betreffend Cyber-Sicherheit und Resilienz und die damit verbundene Einführung geeigneter und verhältnismässiger, technischer und organisatorischer Sicherheitsanforderungen für Cyber-Sicherheit und Resilienz für Unternehmen des Stromsektors Schweiz. Dieses Handlungsfeld wird nachfolgend «Rahmenbedingungen» genannt und entspricht NCS Massnahme 8 «Evaluierung und Einführung von Minimalstandards», sowie dem Beschluss des Bundesrates auf Basis der Empfehlungen der Expertengruppe «Zukunft Datenschutz und Datensicherheit»[75].

Kapitel 4.2 – Überprüfung

Die Überprüfung umfasst Massnahmen zur getreuen Umsetzung bestehender Cyber-Regulierungen durch die Marktteilnehmer des Stromsektors Schweiz. Dieses Handlungsfeld basiert auf dem Entschluss des Bundesrats, dass, entlang von NCS Massnahme 8, verpflichtende Sicherheitsstandards zu prüfen und bis Ende 2022 Lösungsoptionen aufzuzeigen sind.

Kapitel 4.3 – Meldewesen

Das Meldewesen betreffend laufende Cyber-Attacken innerhalb des Stromsektors Schweiz. Dies beinhaltet die Einführung einer Meldepflicht gemäss NCS Massnahme 9 «Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung».

Kapitel 4.4 – Wissensaustausch

Der laufende Wissensaustausch betreffend aktuelle Cyber-Gefahren (Threat Intelligence) innerhalb des Schweizer Stromsektors, sowie auf internationaler Ebene. NCS Massnahme 4 «Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage» wird dadurch für den Stromsektor konkretisiert.

---

[75] Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit (2018), Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit.

4.1 Rahmenbedingungen

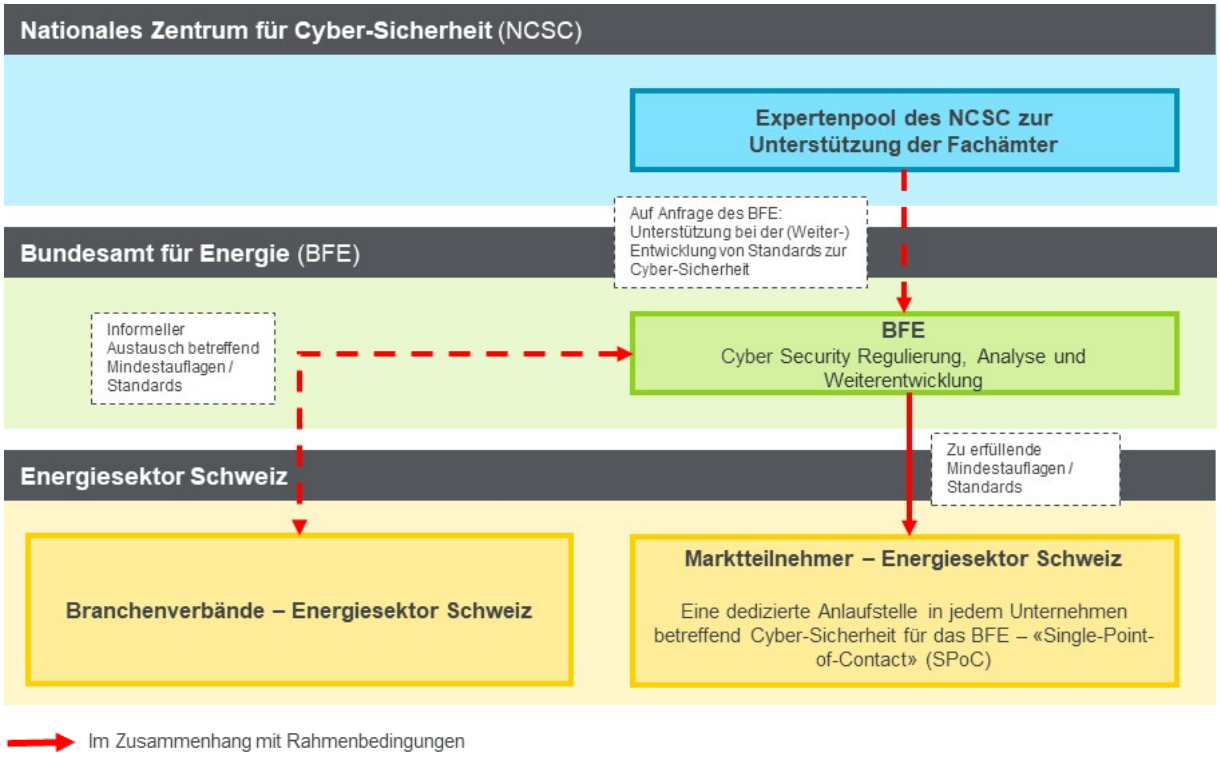


Abbildung 12: Rahmenbedingungen

Die Auswertung der E-Survey zeigt, dass trotz jahrelanger Bemühungen und Hilfestellungen – beispielsweise durch die Einführung eines unverbindlichen IT-/OT-Minimalstandards für Cyber-Sicherheit im Jahr 2018 gemäss der NCS Massnahme 8 – der aktuelle Stand betreffend Cyber-Sicherheit im Stromsektor Schweiz weiterhin bedenklich ist. In Anbetracht der stark durch den technologischen Fortschritt insbesondere in der Digitalisierung getriebenen, schnell wachsenden und sich verändernden Cyber-Gefahrenlandschaft erscheint der aktuelle Stand als nicht mehr zeitgemäss.

Institutionalisierte Rahmenbedingungen betreffend Cyber-Sicherheit und Resilienz und damit verbunden, die Schaffung verbindlicher und verhältnismässiger Anforderungen sowohl technischer, als auch organisatorischer Natur für Cyber-Sicherheit und Resilienz innerhalb des Stromsektors Schweiz, erscheint unausweichlich, wie auch die Expertengruppe «Zukunft Datenschutz und Datensicherheit» festhielt.

Gemäss dem Grundsatz von Art. 6 Abs. 2 des Energiegesetzes (EnG) lässt sich ableiten, dass der Bund und die Kantone grundsätzlich für die notwendigen Rahmenbedingungen bezüglich einer sicheren Energieversorgung der Schweiz verantwortlich sind. In der oben vorgeschlagenen Abbildung würde das BFE eine Rolle einnehmen, in welcher die Einführung verbindlicher Anforderungen betreffend Cyber-Sicherheit und Resilienz im Stromsektor Schweiz, sowie deren stetige Weiterentwicklung, grundsätzlich in den Kompetenzbereich des Fachamtes fällt.

Das BFE wäre hierfür mit seiner Expertise betreffend Energiewirtschaft und Digitalisierung geradezu prädestiniert. Schon heute hätte das BFE unter Umständen die Kompetenzen, für gewisse Bereiche Vorgaben im Sinne einer Regulierung betreffend Cyber-Sicherheit zu erlassen. So z.B. aufgrund von

Art. 5 Abs. 6 StromVV, welcher das BFE befugt, technische und administrative Mindestanforderungen an ein sicheres, leistungsfähiges und effizientes Netz festzulegen. Inwieweit diese grundsätzlich bestehende, gesetzliche Befugnis jedoch bereits ausreichend ist für die Vorgaben, welche später noch beschrieben werden, muss eine weiterführende, rechtliche Analyse zeigen, die nicht Bestandteil dieser Arbeit ist.

Zusätzlich wäre dies ist auch mit dem Bundesratsentscheid, dass das BWL und NCSC in Zusammenarbeit mit den jeweiligen Fachämtern, in diesem Kontext das BFE als zuständiges Fachamt für den Stromsektor, verpflichtende Sicherheitsstandards zu prüfen haben und bis Ende 2022 Lösungsoptionen aufzeigen müssen, zu begründen. Hierzu zählen insbesondere die Rahmenbedingungen bezüglich durch Unternehmen des Stromsektors zu erfüllende Mindestauflagen und Standards im Bereich der Cyber-Sicherheit. So hat das BFE in diesem Bereich erste technische und administrative Mindestanforderungen jedoch nur für intelligente Messgeräte definiert, welches aber nur einen kleinen Bereich der Cyber-Sicherheit umfasst.

Die Umsetzung eines risikobasierten Ansatzes, analog zu dem Grundsatz der NCS 2018-2022, wäre hierbei stets bei der Erarbeitung, sowie Weiterentwicklung von gesetzlichen Anforderungen zu respektieren. Ein risikobasierter Ansatz impliziert die Annahme, dass kein vollständiger Schutz vor Cyber-Risiken möglich ist, die Risiken aber soweit behandelt werden können, dass das verbleibende Risiko tragbar ist. Idealerweise sollten zuerst die grössten Cyber-Bedrohungen im Strommarkt adressiert werden.

Risikobasierter Ansatz zur Festlegung gesetzlicher Cyber-Anforderungen

Zu Beginn sollte definiert werden, welche Marktteilnehmer künftig von bestehenden und neuen Anforderungen betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor betroffen sein sollen. Dieser Schritt erscheint als wichtig, da nicht alle Unternehmen innerhalb des Sektors über die gleichen Ressourcen und Mittel verfügen, sowie die Wahrscheinlichkeit und das Ausmass eines möglichen Cyber-Sicherheitsvorfalls je nach Betrieb sehr verschieden ausfallen können. Wie bereits dargestellt in Kapitel 1 ist der Schweizer Strommarkt stark fragmentiert und heterogen. Dem muss die Regulierung entgegnen.

Dieser Bericht zeigt drei Optionen auf, auf der Basis derer grob entschieden werden könnte, welche Marktteilnehmer künftig grundsätzlich reguliert werden sollten. Nach einer kurzen Beschreibung der jeweiligen Option werden die entsprechenden Vor- (+) und Nachteile (-) aufgeführt.

Option 1: Allgemeiner IT- / OT-Grundschutz für alle Marktteilnehmer (kein risikobasierter Ansatz)

Alle Marktteilnehmer des Stromsektors Schweiz würden flächendeckend verpflichtet, die gleichen Mindestanforderungen betreffend Cyber-Sicherheit und Cyber-Resilienz zu erfüllen. Dies bedeutet eine einheitliche Regulierung aller Marktteilnehmer der Schweiz ohne Berücksichtigung des jeweiligen Risikoprofils der betroffenen Unternehmen und ist daher nicht risikobasiert.

+ Einheitliche Grundbasis an Cyber-Sicherheit und Cyber-Resilienz im gesamten Stromsektor Schweiz
- Widerspricht einem risikobasierten Regulierungsansatz – potentiell unverhältnismässig strenge und entsprechend aufwändige und kostspielige Sicherheitsmassnahmen gegenüber kleineren Marktteilnehmern
- Sehr hoher Überwachungs- und Überprüfungsaufwand betreffend Einhaltung bestehender Cyber-Regulierungen

Option 2: Selektive Schutzanforderungen für relevante Marktteilnehmer (risikobasierter Ansatz)

Diese Option würde die Schaffung gesetzlicher Definitionen inklusive Kriterien und/oder Schwellenwerte umfassen, ab wann Unternehmen im Energiesektor Schweiz jeweils unter gewisse Cyber-Regulierung des BFE fallen. Hierbei sollte das BFE im Rahmen der Regulierung verankern, an welche Unternehmen des Stromsektors Schweiz sich welche Anforderungen jeweils richten – ein gewisser Anteil der Marktteilnehmer könnte daher beispielsweise auch bewusst nicht reguliert sein. Diese Option wäre risikobasiert, da damit die grössten Cyber-Risiken im Sektor angemessen und gezielt vermindert werden könnten.

+ Möglichkeit zur Berücksichtigung der Relevanz einer Unternehmung, beispielsweise unter dem Gesichtspunkt der Risiko- und Gefahrenprofile in Bezug auf die Versorgungssicherheit der Schweiz, d.h. auf die Bereitstellung «kritischer Infrastruktur»
+ Signifikant kleinerer Überwachungs- und Überprüfungsaufwand als in Option 1
+ Erprobter Ansatz in den Nachbarstaaten. Beispiele betreffend mögliche Kriterien / Schwellenwerte für Markteilnehmer-Typen der Nachbarstaaten können als Referenz für die Anpassung auf den Schweizer Markt dienen
+ Risikobasierter Ansatz. Kleinere Unternehmen werden nicht verpflichtet, unverhältnismässig hohe Anforderungen zu erfüllen, verfügen aber trotzdem über einen gewissen Cyber-Grundschutz
- Nicht verpflichtete Marktteilnehmer vernachlässigen potentiell ihre Cyber-Sicherheit und müssen bei einer künftigen, allfälligen Änderung des Regulierungsrahmens einen massiven Rückstand nachholen, sofern nicht andere Massnahmen dies abdämpfen
- Aufgrund der potentiellen Vernachlässigung der Cyber-Sicherheit bei nicht regulierten Marktteilnehmern können sich kaskadenförmige Effekte ergeben. Regulierte Unternehmen, welche aufgrund ihrer Verpflichtungen eigentlich gut gesichert sind, könnten durch die Vernetzung der IT/OT Systeme von Unternehmen ohne Regulierung trotzdem geschwächt werden («Backspill» Effekt)
- Zusätzliche Komplexität und Aufwand für Schaffung sinnvoller Definitionen inklusive Kriterien und/oder Schwellenwerte

Option 3: Allgemeiner Grundschutz für alle mit zusätzlichen Anforderungen für gewisse Betriebe (risikobasierter Ansatz)

Die dritte Option würde die beiden Optionen 1 und 2 kombinieren. Es würden in einem ersten Schritt gewisse, bewusst tief angesetzte Cyber-Grundschutzanforderungen für alle Marktteilnehmer als verbindlich definiert. Über die Zeit würden zusätzlich erhöhte Anforderungen für gewisse Marktteilnehmer gelten, die anhand bestimmter Kriterien wie beispielsweise Unternehmensgrösse, Cyber-Risiken- und Gefahrenlandschaft, etc. identifiziert werden müssten. Das könnte beispielsweise bedeuten, dass für alle KI-Betreiber weiterführende, strengere Massnahmen vorgegeben werden. Auch könnten unter anderem etwa strengere Regeln für Akteure innerhalb der Netzebenen 1-3 gelten, als für Messstellendienstleister.

+ Einheitliches Niveau für Cyber-Sicherheit und Cyber-Resilienz im gesamten Stromsektor Schweiz

+ Risikobasierter Ansatz. Es herrschen zwar Grundschutzanforderungen für alle, jedoch existieren ebenfalls zusätzliche Schutzanforderungen für strategisch relevante Marktteilnehmer basierend auf ihrem Risiken- und Gefahrenprofil durch selektive, zusätzliche Verpflichtungen
- Hohe Komplexität und Aufwand für Schaffung sinnvoller, gesetzlicher Definitionen inklusive Kriterien und/oder Schwellenwerte
- Sehr hoher Überwachungs- und Überprüfungsaufwand betreffend Einhaltung bestehender Cyber-Regulierungen

Empfehlung Option 2
Selektive Schutzanforderungen für relevante Marktteilnehmer

Es wird Option 2 als sinnvolle Vorgehensweise für die Schweiz empfohlen unter der Berücksichtigung von Implementationsaufwand, Ressourceneffizienz und Bewährtheit in anderen Ländern. Eine solche Verpflichtung ist nicht nur möglich, sondern auch sinnvoll und zollt der Heterogenität der Unternehmen der Schweizer Elektrizitätswirtschaft genügend Tribut.

Gemäss Vorschlag sind für alle Regulierungsbereiche (Grundschutz, weiterführende Verpflichtungen, Meldepflicht, etc.) jeweils klare Kriterien und Schwellenwerte zu erarbeiten, anhand von welchen gewisse Unternehmen bestimmten Regulierungen jeweils unterliegen (bspw. für Betreiber kritischer Infrastrukturen, für Akteure innerhalb der Netzebenen 1-3, Anbieter gewisser Dienstleistungen, Marktteilnehmer ab einer gewissen Grösse, Produzenten mit einer gewissen Mindestproduktion, etc.).

Grundlagen für die Erarbeitung gesetzlich verpflichtender Cyber-Anforderungen

Bei der Erarbeitung gesetzlicher verpflichtender Cyber-Anforderungen sollte man sich grundsätzlich stets zuerst an bereits bestehenden, nationalen und kantonalen Regulierungen orientieren und diese sinnvoll harmonisieren und/oder referenzieren. Wenn immer möglich sollte auch eine Referenzierung mit internationalen Frameworks und Standards in Betracht gezogen werden.

Bei der Erarbeitung verpflichtender Cyber-Anforderungen für den Stromsektor Schweiz sollte schrittweise herangegangen werden.

I. In einem ersten Schritt sollte sichergestellt werden, dass ein gewisser Cyber-Grundschutz für relevante Marktteilnehmer im Schweizer Stromsektor gegeben ist. Hierzu sollten unter anderem auch bereits verfügbare Grundlagen im Bereich der Risikoanalyse berücksichtigt werden (existierende Schutzbedarfs- und Risikoanalysen, Inventar kritischer Infrastrukturen des Bundes, etc.).
II. In einem zweiten Schritt sollte eine Harmonisierung und Weiterentwicklung der cyber-relevanten Anforderungen für Betreiber kritischer Infrastrukturen innerhalb des Stromsektors Schweiz ins Auge gefasst werden, da diese aus einer Risikobetrachtung das grösste Gefahrenpotential für den Schweizer Stromsektor darstellen.
III. Sind diese beiden Kategorien zufriedenstellend reguliert, so empfiehlt es sich weiterführenden, Stromsektor-spezifischen Anforderungen zu widmen, welche über den gewünschten Grundschutz herausgehen.

Bei der ersten Stufe – dem Setzen von Cyber-Grundschutz Anforderungen – sollte als initiale Ausgangslage zuerst evaluiert werden, welches Maturitätsniveau betreffend Cyber-Sicherheit und Resilienz die

Unternehmen des Sektors künftig idealerweise erreichen sollten. Dieser Wert kann anschliessend beispielsweise dazu verwendet werden, um bei der Schaffung neuer Anforderungen jeweils zu evaluieren, ob die gewählten Anforderungen dieses Maturitätsziel zu unterstützen vermögen oder möglicherweise sogar zu hoch angesetzt wurden.

Zudem begünstigt das Vorhandensein solch einer Maturitätszielsetzung auch ein einfacheres, künftiges Messen der erzielten Fortschritte innerhalb des Sektors, indem aktuelle Maturitätseinschätzungen der gewählten Zielsetzung künftig gegenübergestellt werden können – so könnten beispielsweise die Selbsteinschätzungsresultate betreffend aktuelle Maturität der in dieser Arbeit präsentierten E-Survey künftig der Maturitätszielsetzung gegenübergestellt werden.

Zur Festlegung solch eines Zielwerts betreffend zu erreichende Maturität schlägt dieser Bericht die folgende Herangehensweise vor:

1. Wie in der NCS 2018-2022 festgehalten wurde, sollte dies gemäss einem risikobasierten Ansatz geschehen. Es sollte daher zunächst der «Risikoappetit» betreffend Cyber- und mögliche Ausfall-Risiken (Resilienz) für den Schweizer Stromsektor definiert werden. Eine «Nulltoleranz» wäre hierbei nicht zielführend – es gilt die Annahme, dass ein vollständiger Schutz vor Cyber-Risiken grundsätzlich nicht möglich ist. Vorhandene Cyber- und Resilienz-Risiken des Sektors sollten daher künftig soweit mittels regulatorischer Anforderungen mitigiert werden, bis das verbleibende Restrisiko aus Sicht des Regulators tragbar ist (= «Risikoappetit»).
2. In einem zweiten Schritt gilt es zu ermittelten, welches Ziel-Maturitätsniveau (= IKT «Implementation Tier» / «Stufe» - mögliche Werte 1-4, siehe Anhang 1) es jeweils für die verschiedenen Cyber-Fähigkeiten entlang des IKT-Minimalstandards des Bundes zu erreichen gilt um dem gewählten «Risikoappetit» gerecht zu werden (es existieren insgesamt 108 IKT Cyber-Fähigkeiten – siehe Anhang 1). Der gesetzte Durchschnittswert betreffend Ziel-Maturitätsniveau über alle 108 Cyber-Fähigkeiten entspricht dem Gesamtzielwert betreffend Cyber-Maturität für den Sektor.

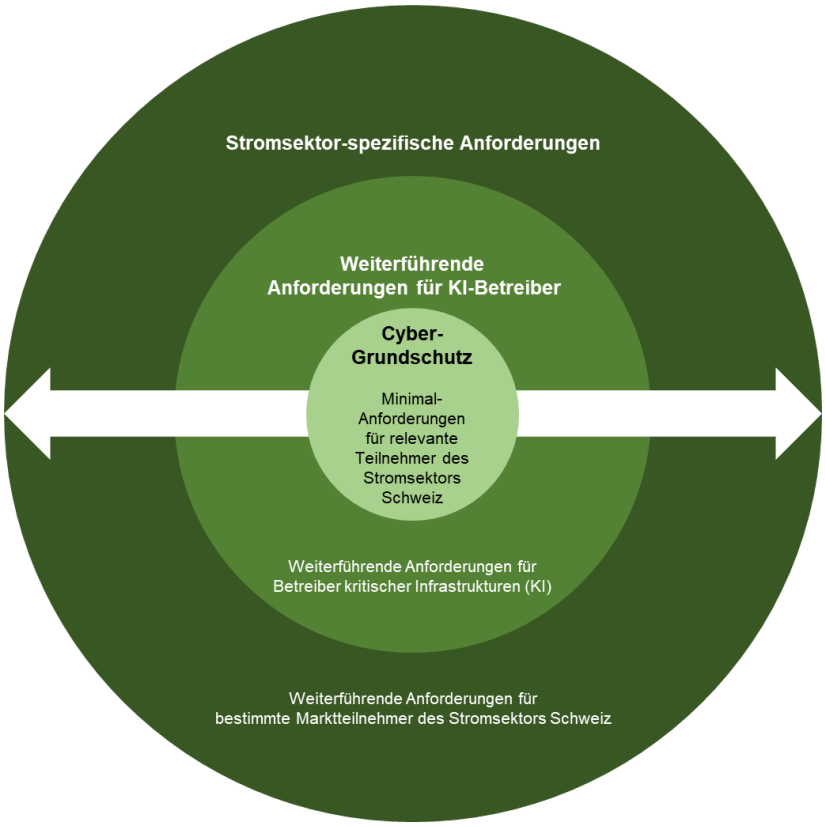


Abbildung 13: Erarbeitung gesetzlich verpflichtender Cyber-Anforderungen

Tabelle 9: Etappierung und Strukturierung der Vorgaben einer Regulierung zur Cyber-Sicherheit

Kategorie	Beschreibung und Empfehlung	Nationale Grundlagen	Internationale Frameworks und Standards
Cyber-Grundschutz Minimal-Anforderungen für relevante Teilnehmer des Stromsektors Schweiz	Bei der Erstellung von Mindestanforderungen sollte nebst Orientierung am IKT Minimalstandard des Bundes beispielsweise der Bereich (Cyber-) «Risikomanagement» als eines der ersten Themen zwingend vertieft mitabgehandelt werden. Beispielsweise könnte der internationale Standard ISO 27001 zur zwingenden Einführung eines Informationssicherheits-Managementsystems (ISMS) für die relevanten Marktteilnehmer angedacht werden. Dieser wäre ebenfalls in der Lage bereits grosse Teile der Anforderungen des IKT Minimalstandards abdecken.	- IKT Minimalstandard (welcher bereits auf internationaler Ebene existierende Frameworks referenziert)	- ISO/IEC 27001 (zertifizierbarer, internationaler Standard) - NIST Publikation 800-30 Rev. 1 (Risikomanagement für Informationssysteme) - CRAMM Risikomanagement Methodologie - OCTAVE, Werkzeuge, Techniken und Methoden - FAIR, Methodologie zur Quantifizierung und Management von Risiken - IRAM2, Ansatz für die Risikoanalyse - MAGERIT, Methodologie für Risikoanalyse und Risikomanagement - MEHARI, Methoden für Risikoanalyse und Risikomanagement - MONARC, Methodologie für Risikomanagement
Cyber-Anforderungen für KI-Betreiber Weiterführende Cyber-Anforderungen für Betreiber kritischer Infrastrukturen (KI) *bspw. für Betreiber von Atomkraftwerken, Staudämmen, kritischen Netzknotenpunkten, etc.*	Primär sollte man sich an bereits bestehenden, sicherheitsrelevanten SKI-Anforderungen in den verschiedensten Gesetzgebungen des Bundes und der Kantone orientieren. Zusätzlich wird empfohlen, sich an den rechts aufgeführten, weiterführenden internationalen Frameworks und Standards orientieren.	- bestehenden Sicherheitsvorgaben für KI-Betreiber innerhalb bestehender Regulierungen des Bundes und der Kantone *bspw. Strahlenschutzgesetz StSG, Kernenergiegesetz KEG, Stauanlagengesetz, Verordnung des UVEK über die Gefährdungsmassnahmen und Sicherheitsmassnahmen für Kernanlagen und Kernmaterialien, etc.*	- NIST Framework für die Verbesserung von Critical Infrastructure Cybersecurity - NERC CIP–002 bis CIP-011 Critical Infrastructure Protection Cyber Security - ANSI/ISA, Series ISA-62443: Security for industrial automation and control system

Kategorie	Beschreibung und Empfehlung	Nationale Grundlagen	Internationale Frameworks und Standards
Stromsektor-spezifische Anforderungen zu Cyber-Sicherheit Weiterführende Anforderungen für bestimmte Marktteilnehmer des Stromsektors Schweiz *bspw. für Akteure innerhalb der Netzebenen 1-3, Anbieter gewisser Dienstleistungen, Marktteilnehmer ab einer gewissen Grösse, Produzenten mit einer gewissen Mindestproduktion, etc.*	Es wird empfohlen, sich bei der Verankerung stromspezifischer Anforderungen zu Cyber-Sicherheit primär an den bereits bestehenden sicherheitsspezifischen Anforderungen des Bundes innerhalb des Stromsektors Schweiz zu orientieren, sowie dem OT-Handbuch des Verbands Schweizerischer Elektrounternehmen (VSE). Zusätzlich wird empfohlen sich an den rechts aufgeführten, weiterführenden internationalen Frameworks und Standards orientieren. *Wichtig:* *Dabei sollten bestehende Überlappungen und Unklarheiten in der derzeit fragmentierten Vorgabenlandschaft ausgeräumt werden und neue, weitergehende Anforderungen mit dem Grundschutz und dem KI-Schutz jeweils eng abgestimmt sein.*	- Sicherheitsrelevante Weisungen des BFE, der ElCom, des ENSI und des ESTI - OT-Handbuch des Verbands Schweizerischer Elektrounternehmen (VSE) - Bestehende Branchenrichtlinien *bspw. Richtlinien für die Datensicherheit von intelligenten Messsystemen, standardisierter Datenaustausch für den Strommarkt Schweiz, Data Policy in der Energiebranche (vgl. Anhang 4).*	- ISO 27019 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry - NISTIR 7628 Guidelines for Smart Grid Cybersecurity - NIST Industrial Control Systems (ICS) Security - IEEE STANDARD 1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security - IEC 61850 Power Utility Automation

Bemerkung: Diese vorgeschlagene regulatorische Entwicklung ist entlang von unterschiedlichen Geschehnissen in anderen Bundesämtern des UVEK einzuordnen.

Beispielsweise wird in der neuen Ausgabe der Ausführungsbestimmungen zur Eisenbahnverordnung (EBV), welche vom BAV im November 2020 herausgegeben wurde, festgehalten, dass Anlagen, Systeme und Fahrzeuge, die IKT-Systeme verwenden oder enthalten, verhältnismässig gegen missbräuchliche Eingriffe geschützt werden müssen. Zur Beherrschung der Risiken soll ein ISMS eingerichtet und instandgehalten werden. Die Konformität mit ISO 27001 und wo relevant mit IEC 62443 "Industrial communication networks - IT security for networks and systems" ist anzustreben.

Ebenso wurde im Aufgabenbereich der BAKOM in einer revidierten Fassung des Fernmeldegesetzt (FMG) im Januar 2021 verordnet, dass die Anbieterinnen von Fernmeldediensten unbefugte Manipulation durch fernmeldetechnische Übertragungen bekämpfen müssen, Art. 48a FMG.

4.2 Überprüfung

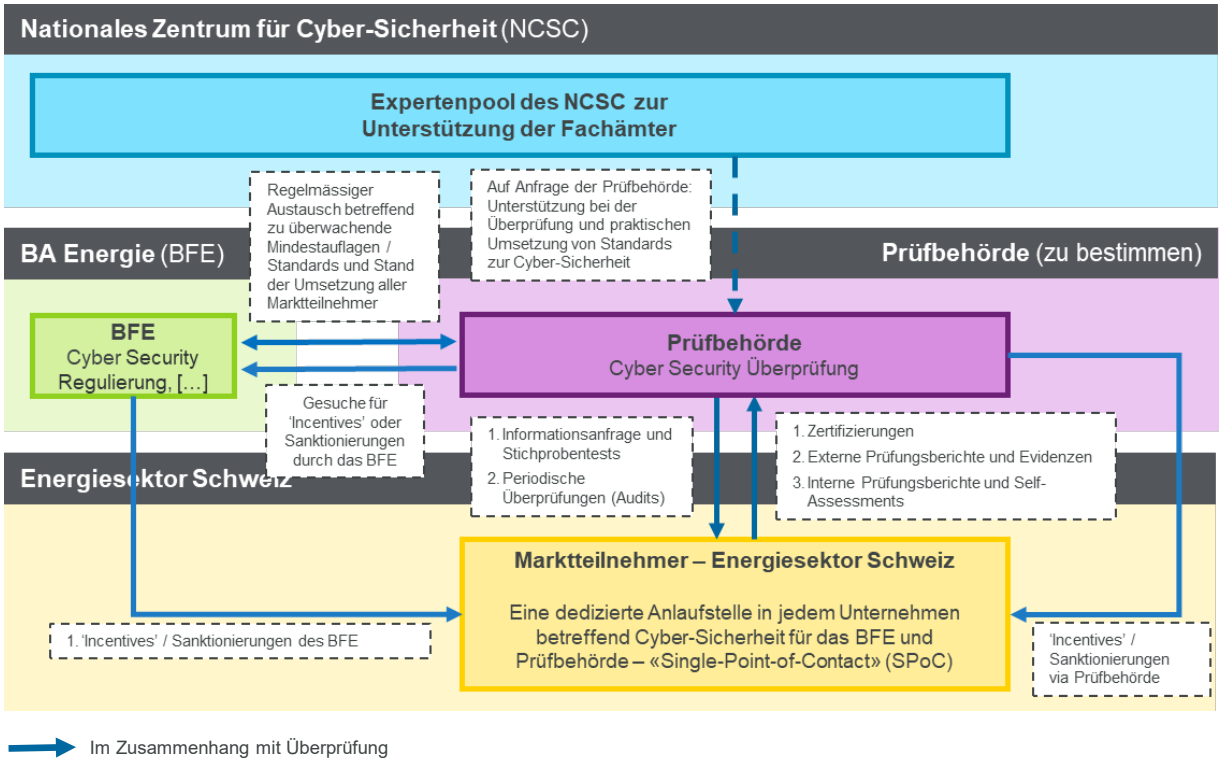


Abbildung 14: Überprüfung

Analog zu den Überlegungen zu einer Verpflichtung der Marktteilnehmer des Stromsektors Schweiz zur Einhaltung gesetzlich verpflichtender Anforderungen, sollten Mechanismen institutionalisiert werden, welche die Einhaltung und adäquate Umsetzung dieser Vorgaben auf regelmässiger Basis überprüfen.

Dieser Bericht empfiehlt, dass eine Prüfbehörde als Mandatsträgerin für künftige Cyber-Überprüfungen agieren würde und somit als überwachende Instanz für Konformität mit geltenden Regulierungen betreffend Cyber-Sicherheit im Schweizer Stromsektor etabliert würde.

Für die erfolgreiche Wahrnehmung dieser Aufgaben durch die Prüfbehörde würde es unterschiedliche Kompetenzen und Überprüfmechanismen benötigen. Der vorliegende Bericht behandelt in diesem Kapitel unter anderem auch mögliche Überprüfungsmechanismen, welche gemäss der oben vorgeschlagenen Abbildung für die Schweiz alle in Kombination ihre Anwendung finden sollten. Diese wären:

- Initiale Registrierung
- Überprüfung (Audit)
- Stichprobenkontrollen
- Selbstbeurteilungen
- Zertifizierungen
- 'Incentives' / Sanktionierungen

Bestimmung der Prüfbehörde

Mit dem dargestellten Vorschlag würde eine noch zu bestimmende Prüfbehörde Mandatsträgerin für künftige Cyber-Überprüfungen und agiert somit als überwachende Instanz für Konformität mit geltenden Regulierungen betreffend Cyber-Sicherheit im Schweizer Stromsektor.

Option 1: BFE als Prüfbehörde (keine dedizierte Prüfbehörde)

Das BFE wäre sowohl zuständig für das Setzen der Rahmenbedingungen, als auch die anschliessende Überprüfung bzw. Aufsicht.

Es existieren bereits gewisse Analogien, so z.B. im Bereich von Stauanlagen, Talsperren und Rohrleitungen, wo das BFE heute bereits sowohl regulierende als auch überprüfende Aufgaben wahrnimmt. Ein Aufsichtsmandat für technische Sicherheit und Compliance wird vom BFE aktuell bereits für 200 bestehende Anlagen umgesetzt. Als Aufsichtsbehörde beurteilt das BFE eingereichte Berichte und kontrolliert, ob die Anforderungen an die technische Sicherheit eingehalten werden. Auch führt das BFE bei den Anlagen periodisch Kontrollen durch (siehe StAG Art.8).

+ BFE übernimmt bereits heute teilweise Aufgaben, welche sowohl in den Bereich der Aufsicht, als auch in die anschliessende Überprüfung fallen
+ Ein gewisses Fachwissen im Bereich Cyber-Sicherheit und Digitalisierung ist beim BFE bereits vorhanden, jedoch ausbaubedürftig
+ Das BFE verfügt über gewisse Sanktionierungs- und 'Incentivierungs'-Kompetenzen und ist bereits heute zuständige Instanz bei Verstössen gegen das StromVG
- Keine klare Gewaltentrennung zwischen regulierender und überprüfender Instanz
- Entspricht derzeit nicht dem aktuellen Mandat des BFE im Bereich der Stromversorgung
- Dieser Ansatz würde vermehrt zu Kompetenz-Abgrenzungsfragen zwischen dem BFE und den aktuellen Tätigkeiten der ElCom führen

Option 2: ElCom als Prüfbehörde (dedizierte Prüfbehörde)

Eine klare Aufteilung der Kompetenzen zwischen dem BFE und der ElCom als eine dedizierte Prüfbehörde.

Das Mandat der Prüfbehörde entspricht in gewissen Teilen dem bereits heute bestehenden Mandat der ElCom. Sie ist schon heute die Einhaltung des Stromversorgungs- und Energiegesetzes für Netzbetreiber überwacht was sich aus Art.22 Abs.3 StromVG hergeleitet.

+ Entspricht bereits heute teilwiese dem aktuellen Mandat der ElCom, welche für die Überwachung der Einhaltung des StromVG durch Netzbetreiber zuständig ist
+ Die ElCom verfügt bereits heute über gewisse Kompetenzen, Prozesse und Mechanismen, welche sich künftig für eine überwachende Funktion betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor weiterverwenden lassen würden
+ Klare Gewaltentrennung zwischen der regulierenden, sowie der überwachenden Instanz
+ Die ElCom verfügt bereits über detaillierte Branchekenntnisse, ist mit einem Grossteil der Marktteilnehmer gut vernetzt und eingespielt (bspw. bereits ein Register und Registrierungsprozess für gewisse Marktteilnehmer vorhanden)

+ Es besteht ein gewisses Fachwissen in dem Bereich der Cyber-Sicherheit und darüber hinaus im Bereich der Krisenprävention
- Gewisse Doppelspurigkeiten mit dem aktuellen Mandat des Eidgenössischen Instituts für Metrologie (METAS). Das METAS nimmt derzeit überprüfende Tätigkeiten im Sinne der hier vorgeschlagenen Prüfbehörde wahr, indem es unter Zuhilfenahme externer Experten die Einhaltung von sicherheitstechnischen Anforderungen an die Messkette (Smart Meter, nachgelagerte IT-Systeme sowie Schnittstellen) sicherstellt

Option 3: Eidgenössisches Institut für Metrologie als Prüfbehörde (dedizierte Prüfbehörde)

Eine klare Aufteilung der Kompetenzen zwischen dem BFE und dem Eidgenössischen Institut für Metrologie (METAS) als eine dedizierte Prüfbehörde.

Das METAS hat gemäss den Vorgaben von Art.8b StromVV seit 2018 ein Mandat als Prüf- und Zertifizierungsbehörde im Zusammenhang von sicherheitstechnischen Anforderungen für Smart Meter mit Herstellern und Betreibern bzw. Unternehmen der Elektrizitätswirtschaft. Das METAS erfüllt dabei daher bereits teilweise Aufgaben einer Cyber-Sicherheitsbehörde.

+ Entspricht bereits heute teilwiese dem aktuellen Mandat des METAS, welches für die Überwachung der Einhaltung von sicherheitstechnischen Anforderungen an Smart Meter zuständig ist
+ Das METAS verfügt bereits heute über gewisse Kompetenzen, Prozesse und Mechanismen, welche sich künftig für eine überwachende Funktion betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor weiterverwenden lassen würden
+ Klare Gewaltentrennung zwischen der regulierenden, sowie der überwachenden Instanz
+ Das METAS verfügt bereits über detaillierte Kenntnisse, in einem Teilbereich der Cyber-Sicherheit innerhalb des Schweizer Stromsektors und ist mit einem Grossteil der Marktteilnehmer bereits gut vernetzt und eingespielt
+ Das METAS ist bereits in engem Austausch mit anderen (internationalen) Prüfstellen, welche auf Basis von Industriestandards digitale Geräte und Systeme auf Cyber-Sicherheit hin prüfen
- Es besteht ein grösseres Fachwissen im Bereich der Cyber-Sicherheit innerhalb des METAS, jedoch benötigtes es noch eine deutliche Ausweitung der aktuellen Kenntnisse und Kompetenzen
- Gewisse Doppelspurigkeiten mit dem aktuellen Mandat der ElCom, welche aktuell bereits für überprüfende Tätigkeiten betreffend die Einhaltung des StromVG durch Netzbetreiber zuständig ist

Empfehlung Option 2 oder 3
Eine dedizierte Prüfbehörde

Es werden Optionen 2 oder 3 als sinnvolle Vorgehensweise für die Schweiz empfohlen. Eine separierte Behörde als Prüfbehörde sichert eine Gewaltentrennung zwischen der regulierenden, sowie der überwachenden Instanz. Beide Optionen entsprechen bereits heute teilweise den aktuellen Mandaten, was den zukünftigen Implementationsaufwand vereinfachen würde. Ebenso bestehen schon gewisse Kompetenzen, Prozesse und Mechanismen bei der ElCom und METAS um eine solche Tätigkeit auch auszuüben.

Hierbei würde sich besonders eine nähere Betrachtung der ElCom als künftige Prüfbehörde anbieten. Dies unter Berücksichtigung des bereits aktuell bestehenden Mandats der ElCom betreffend die Einhaltung des StromVG durch Netzbetreiber, sowie deren bereits vorhandene Kompetenzen, Prozesse und Mechanismen, welche sich künftig gut für eine überwachende Funktion betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor weiterverwenden lassen würden.

Welche Option letzten Endes gewählt werden sollte, sollte sich jedoch auf eine vertiefte Abklärung (inklusive der rechtlichen Aspekte) abstützen und konnte hier im Zusammenhang mit dieser Arbeit nicht abschliessend ermittelt werden.

Initiale Registrierung

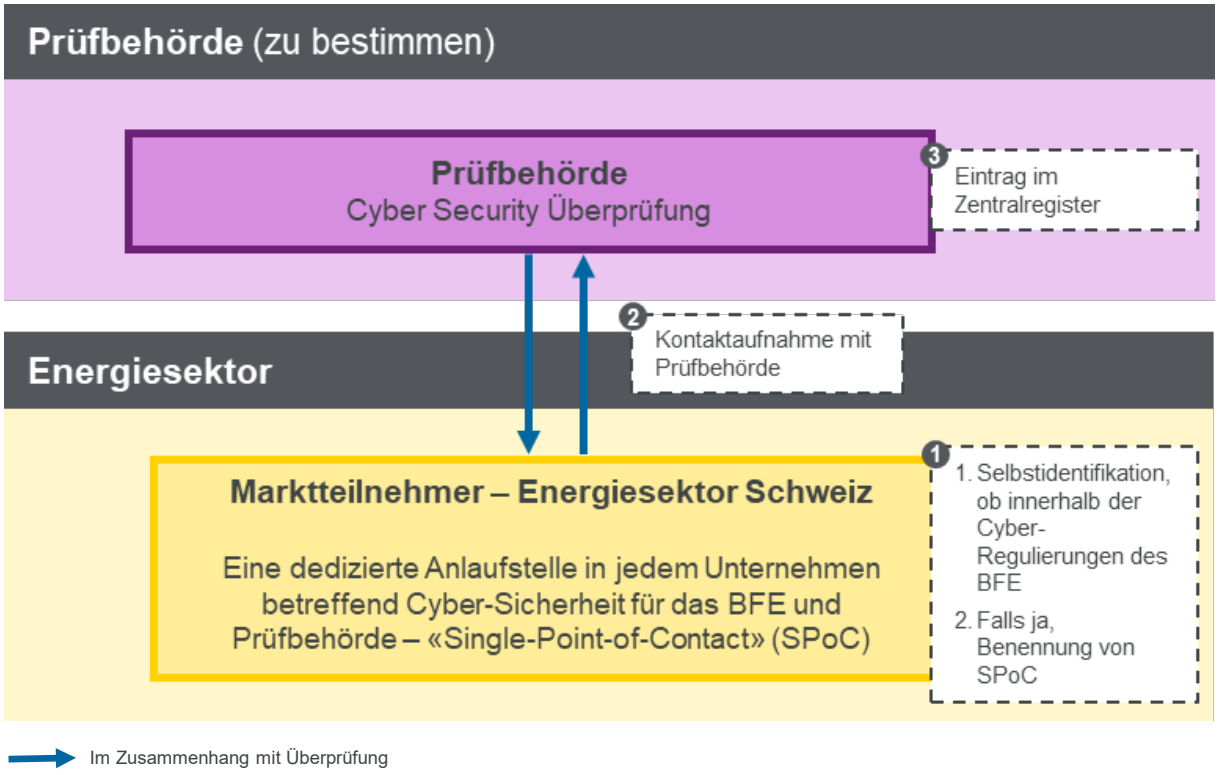


Abbildung 15: Initiale Registrierung

Für die ordnungsgemässe Einrichtung und Ausübung der Überwachungs- und Überprüfungsfunktion der Prüfbehörde bräuchte es eine vollständige Übersicht aller Marktteilnehmer des Schweizer Stromsektors, welche aktuell geltende Cyber-Regulierungen des Bundes zu erfüllen haben. Dies sollte idealerweise in der Form eines zentralen Registrierungsprozesses und zentral geführten Registers geschehen.

Es wird in diesem Bericht vorgeschlagen, eine gesetzliche Registrierungspflicht für alle cyber-regulierten Marktteilnehmer des Strommarktes Schweiz zu verankern. Unternehmen wären daher verpflichtet selbst regelmässig zu überprüfen, ob und inwiefern sie unter die aktuellen Cyber-Regulierungen fallen würden. Falls ja, so müssten diese sich selbstständig bei der Prüfbehörde melden und entsprechen

registrieren. Geschieht dies nicht, so würde bei Entdecken dieses Versäumnisses entsprechend eine Strafe drohen.

Die Prüfbehörde müsste im Gegenzug die Einrichtung entsprechender Registrierungsprozesse und das Führen solch eines zentralen Registers sicherstellen. Es ist hierbei anzumerken, dass auf Seiten ElCom bereits heute ein Register aller Schweizer Netzbetreiber und gewisser Marktteilnehmer im Bereich Stromhandel im Rahmen ihrer derzeitigen Überwachungsaufgaben geführt wird. Der Schwerpunkt dieser Aufsichtstätigkeiten liegt allerdings insbesondere auf der Überwachung der Netzkosten und Netztarifen, sowie auf dem Aufdecken von allfälligem Insiderhandel und potentieller Marktmanipulationen.

Im Register könnten nebst den allgemeinen Informationen betreffend des zu registrierenden Unternehmens zusätzlich noch weitere Informationen erfasst und künftig gepflegt werden. Ein Beispiel hierfür wären etwa das zentrale Pflegen weiterführender Informationen betreffend welche der bestehenden Cyber-Vorgaben das betroffene Unternehmen jeweils konkret zu erfüllen hat.

Auch die regelmässige Nachpflege der jeweiligen Kontaktangaben des «Single Point of Contact» (SPoC) des Unternehmens könnte in diesem Register mitgeführt werden. Das Bereitstellen eines dedizierten Ansprechpartners jedes Unternehmens für das BFE und die Prüfbehörde betreffend Cyber-Sicherheit, würde eine Zusammenarbeit der verschiedenen Akteure vereinfachen und zeitgleich sicherstellen, dass die entsprechenden Verantwortlichkeiten innerhalb der regulierten Unternehmen definiert wären. Die Einsetzung des «SPoCs» durch alle Unternehmen des Stromsektors Schweiz sollte entsprechend ebenfalls als eine sogenannte Mindestanforderung im Rahmen einer Regulierung verankert werden.

Eine solche gesetzliche Anforderung wäre im Grundsatz nichts Neues für die Unternehmen. Eine bereits bestehende Analogie für diesen «SPoC»-Ansatz ist beispielsweise die Ernennung eines betrieblichen Datenschutzverantwortlichen. Im Rahmen des revidierten Bundesgesetzes über den Datenschutz von 2008, können Unternehmen einen internen Datenschutzverantwortlichen ernennen und den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) entsprechend darüber in Kenntnis setzen.

Das Register könnte zudem als Koordinationsinstrument für die Überprüfungsaktivitäten der Prüfbehörde dienen. So könnten beispielsweise ebenfalls alle bereits vorhandenen Überprüfungsresultate, sowie der aktuelle Stand des Nachweises für die derzeitige Einhaltung der gemachten Cyber-Vorgaben jeweils für die betroffenen Unternehmen zentral mitgeführt werden. Auch Informationen betreffend erhaltene Sanktionierungen oder ‘Incentivierungen’ könnten zentral erfasst sein.

Anhand dieser Daten könnten ebenfalls verschiedene Risikoprofile der Marktteilnehmer definiert werden, welche anschliessend beispielsweise die Art der Überprüfungstätigkeiten (umfassende Überprüfung, Stichprobenkontrollen, Selbstüberprüfung, etc.), sowie die Periodizität der jeweiligen Überprüfungstätigkeiten bestimmen (bspw. jährlich, alle vier Jahre, etc.).

Empfehlung betreffend im Zentralregister zu führender Informationen

In einem zentral geführten Register sollten idealerweise mindestens die folgenden Informationen von den Unternehmen aufgenommen werden:

- Firma (z.B. Rechtsform und Sitz),
- Eingenommene Marktrollen (Netzbetreiber, Lieferant, Händler, Aggregator, etc.),
- Kontaktdaten des betrieblichen SPoC,
- Risiko-Kategorisierung der Unternehmen (Schwellenwerte),
- zu erfüllende Anforderungen (Grundschutz, Weiterführend, Stromspezifisch)
- Einstufung der letzten Selbstbeurteilung,
- Gelieferte Nachweise für die Einhaltung der Verpflichtungen, und

- Gesprochene ‘Incentivierungen’ / Sanktionierungen,
- Erfolgte Massnahmen bei ‘Incentivierung’ und Sanktionierung.

Überprüfung (Audit)

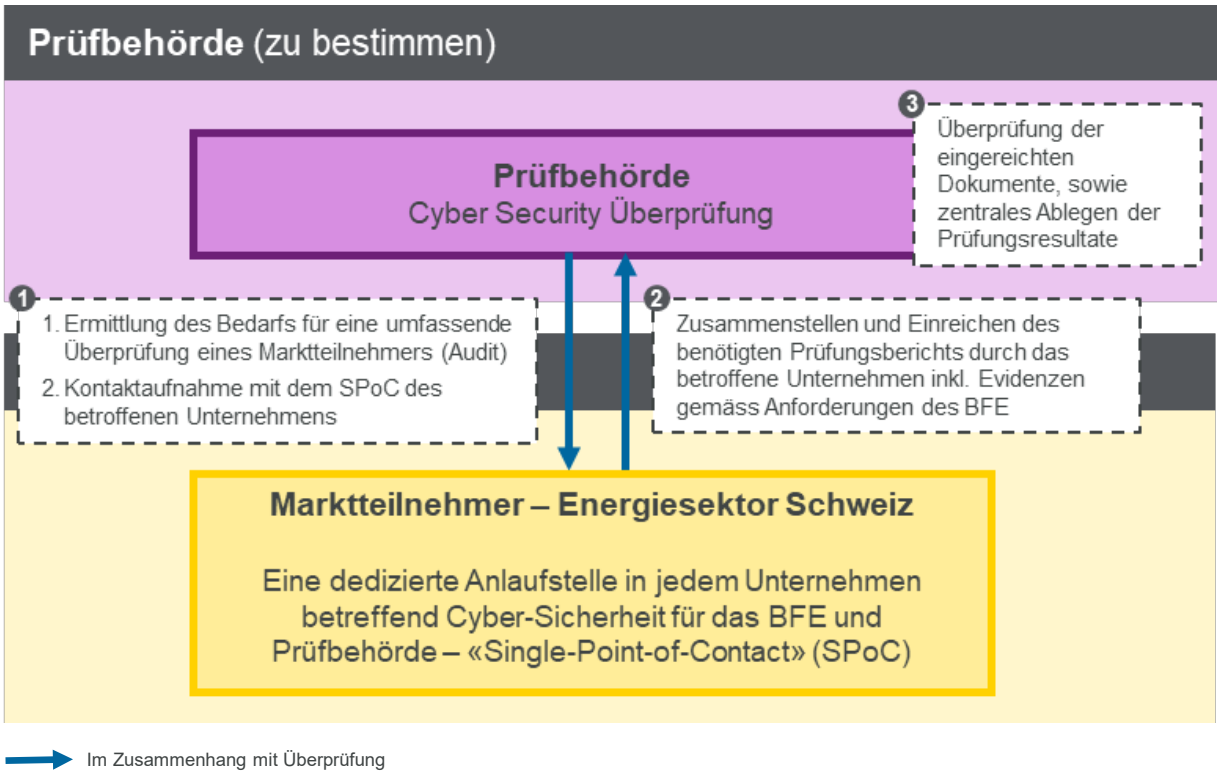


Abbildung 16: Überprüfung (Audit)

Umfassende Überprüfungen (Audits) wären ein zentrales Instrument für die ordnungsgemässe Einrichtung und Ausübung der Überwachungs- und Überprüfungsfunktion der Prüfbehörde. Hierbei sollte jeweils ein holistischer Nachweis durch die betroffenen Marktteilnehmer gegenüber der Prüfbehörde erbracht werden, dass diese mit all den derzeit bestehenden Cyber-Regulierungen in Einklang sind.

Die Prüfbehörde sollte hierbei intern einen risikobasierten Mechanismus entwickeln, um den Bedarf einer Überprüfung eines Markteilnehmers jeweils ermitteln zu können. Beispielsweise könnten anhand verschiedener Risikoprofile von Unternehmen unter anderem die Art der Überprüfungstätigkeiten (umfassende Überprüfung gemäss diesem Kapitel, Stichprobenkontrollen, Selbstüberprüfung, etc.), sowie die Periodizität der jeweiligen Überprüfungstätigkeiten festgelegt werden (bspw. jährlich, alle vier Jahre, etc.). So könnte beispielsweise anstatt auf eine regelmässig wiederkehrende, vollumfängliche Überprüfung für gewisse Markteilnehmer auf ein Modell gesetzt werden, bei welchem die jeweilige Überprüfung auch teilweise auf Basis von Stichprobenkontrollen erfolgen würde.

Würde der Bedarf für eine umfassende Überprüfung (Audit) eines Marktteilnehmers durch die Prüfbehörde ermittelt, so sollte diese gemäss der vorgeschlagenen Abbildung oben direkt den Kontakt mit dem durch das betroffene Unternehmen registrierten «Single Point of Contact» (SPoC) aufnehmen können und das Überprüfungsbegehren entsprechend platzieren können. Eine entsprechende Mitwirkungspflicht der Marktteilnehmer bei Anfragen der Prüfbehörde sollte entsprechend gesetzlich verankert werden.

Der SPoC des betroffenen Marktteilnehmers würde die entsprechende Anfrage intern koordinieren, die hierfür benötigten Evidenzen sammeln und den geforderten Prüfbericht erstellen. Anschliessend würde der SPoC den finalisierten Bericht fristgerecht an die Prüfbehörde zukommen lassen.

Die eingereichten Dokumente würden anschliessend auf Seiten der Prüfbehörde überprüft und Resultate der Überprüfungstätigkeiten im Register abgelegt. Bei einer allfälligen Nichterfüllung gewisser Anforderungen durch den Marktteilnehmer könnten erweiterte Auflagen durch die Prüfbehörde erfolgen und/oder gezielte Sanktionierungen gesprochen werden (siehe späteres Unterkapitel).

Die Prüfbehörde sollte intern über entsprechende Prozesse, Kompetenzen und Ressourcen verfügen, um den allfälligen Aufgaben im Rahmen der Überprüfungstätigkeiten gerecht zu werden. Es gilt jedoch anzumerken, dass grosse Teile der Arbeiten der Prüfbehörde auch externalisiert werden könnten. Die Abläufe zur Überprüfung der durch die Marktteilnehmer eingereichten Prüfberichte und Evidenzen können entweder komplett durch die Prüfbehörde selbst, oder aber teilweise an Drittfirmen externalisiert werden. So könnten externe Dritte entsprechend grosse Teile der anstehenden Arbeitsschritte erledigen und der Prüfbehörde jeweils direkt die ihrerseits festgestellten Lücken / Verstösse mitteilen.

Die Prüfbehörde müsste so also faktisch nur noch die letzten Schritte der Überprüfung durchführen und entsprechend die durch Dritte bereits festgestellten Lücken / Verstösse jeweils von ihrer Seite her noch bestätigen, sowie das Prüfresultat finalisieren und dem betroffenen Unternehmen kommunizieren.

Im Folgenden wird dargestellt, welche Möglichkeiten zur Auslagerung von Aufgaben und Kompetenzen im Bereich der Überprüfung für die Prüfbehörde bestehen. Nach einer kurzen Beschreibung der jeweiligen Option werden die entsprechenden Vor- (+) und Nachteile (-) aufgeführt.

Option 1: Selektive Auslagerung gewisser Überprüfungstätigkeiten für einen Teil der Marktteilnehmer

Bestimmte Marktteilnehmer würden für einen definierten Zeitraum an externe Prüfstellen verwiesen und grösstenteils mittels externer Hilfe überprüft. Beispielsweise könnten die Überprüfungstätigkeiten für die aus Sicht der Prüfbehörde weniger kritischen Bertriebe ausgelagert werden, damit die Prüfbehörde ihren Fokus auf jene Unternehmen setzten kann, welche ein höheres Risikoprofil ausweisen.

+ Ermöglicht die risikobasierte Priorisierung von Marktteilnehmern und die Auslagerung von «weniger problematischen» Überprüftätigkeiten an externe Stellen
+ Ermöglicht einen höheren Grad an Flexibilität für die Prüfbehörde betreffend Einsatz ihrer eigenen, internen Ressourcen
+ Potentielle Möglichkeit zur Einsparung von Personalkosten seitens der Prüfbehörde
- Notwendigkeit zur starken Formalisierung von Standards und Prozessabläufen für die Durchführung der Überprüfungstätigkeiten, sowie Vorlagen und Formate zur Rapportierung und Dokumentation von Prüfergebnissen durch Dritte
- Ein gewisses Mass an Interpretationsspielraum durch Dritte, ob gewisse Evidenzen nun die regulatorischen Anforderungen gemäss Auslegung der Prüfbehörde erfüllen oder nicht. Möglicherweise Notwendigkeit zur Schulung und/oder Akkreditierung des externen Dritten, um sicherstellen zu können, dass dieser die Überprüfungstätigkeiten in der Qualität und mit dem Verständnis der Prüfbehörde durchführen kann
- Ein «gesundes» Mass zwischen Auslagerung und interner Aufgabenverteilung muss gefunden werden, um interne Kompetenzen nachhaltig aufrecht zu erhalten

Option 2: Auslagerung gewisser Überprüfungstätigkeiten für alle Marktteilnehmer

Alle Marktteilnehmer würden jeweils an externe Prüfstellen zugewiesen und grösstenteils mittels externer Hilfe überprüft. Die Prüfbehörde hätte die Möglichkeit parallel gezielte Stichprobenkontrollen durchzuführen, um einen zusätzlichen Fokus auf jene Unternehmen zu setzten, welche ein höheres Risikoprofil ausweisen.

+ Priorisierung der Ressourcen der Prüfbehörde auf die grössten Cyber-Gefahren und Risiken – die Prüfbehörde kann sich mit ihren internen Ressourcen komplett auf durch Dritte gefundene Mängel, sowie der Durchführung gezielter Stichprobenkontrollen konzentrieren
+ Potentielle Möglichkeit zur Einsparung von Personalkosten seitens der Prüfbehörde
- Notwendigkeit zur starken Formalisierung von Standards und Prozessabläufen für die Durchführung der Überprüfungstätigkeiten, sowie Vorlagen und Formate zur Rapportierung und Dokumentation von Prüfergebnissen durch Dritte
- Ein gewisses Mass an Interpretationsspielraum durch Dritte, ob gewisse Evidenzen nun die regulatorischen Anforderungen gemäss Auslegung der Prüfbehörde erfüllen oder nicht. Möglicherweise Notwendigkeit zur Schulung und/oder Akkreditierung des externen Dritten, um sicherstellen zu können, dass dieser die Überprüfungstätigkeiten in der Qualität und mit dem Verständnis der Prüfbehörde durchführen kann

Option 3: Keine Auslagerung der Überprüfungstätigkeiten

Die Prüfbehörde würde die kompletten Überprüfungstätigkeiten mittels interner Ressourcen durchführen und es fände keine Auslagerung an externe Dritte statt.

+ Schnelle Reaktions- und Änderungsmöglichkeiten betreffend der zu verwendenden Prozesse und Methodologie, sowie der eigenen Auslegungsinterpretation, ob gewisse Evidenzen nun die regulatorischen Anforderungen erfüllen oder nicht
+ Zusätzlich gewonnene Erkenntnisse bei der Durchführung der Überprüfungstätigkeiten können direkt mit dem BFE geteilt werden, für eine kontinuierliche Optimierung der regulatorischen Vorgaben betreffend Cyber-Sicherheit
- Grosser Bedarf an internen Ressourcen und Aufbau entsprechender Fachkompetenzen auf Seiten der Prüfbehörde
- Statischer Ressourcenpool und daher Mangel an Flexibilität in Spitzenlast-Situationen («Peaks»)
- Mit hoher Wahrscheinlichkeit teurer als die Auslagerung gewisser Überprüfungstätigkeiten an externe Dritte

Empfehlung Option 1 oder 2
Auslagerung gewisser Überprüfungstätigkeiten an externe Dritte

Grundsätzlich ist eine Überprüfung der Einhaltung der Vorgaben sinnvoll und sollte umgesetzt werden. Nur so kann auch die Wirksamkeit der Vorgaben sichergestellt werden.

Prinzipiell bieten sich die Optionen 1 und 2 für den Schweizer Strommarkt an. Eine Auslagerung würde ermöglichen, dass die Prüfbehörde ihre Prüftätigkeit auf solche Unternehmen fokussieren kann, welche ein höheres Cyber-Risiko- und Gefahrenprofil aufweisen und für die Energieversorgungssicherheit von wesentlicher strategischer Bedeutung sind.

Option 3 erscheint wegen dem hohen, internen Ressourcenbedarf auf Seiten der Prüfbehörde als nicht praktikabel.

Wie im folgenden Unterkapitel dargelegt wird, könnten zudem Stichprobenkontrollen der Prüfbehörde im Rahmen beider empfohlener Optionen als komplementäres Instrument eingesetzt werden.

Stichprobenkontrollen

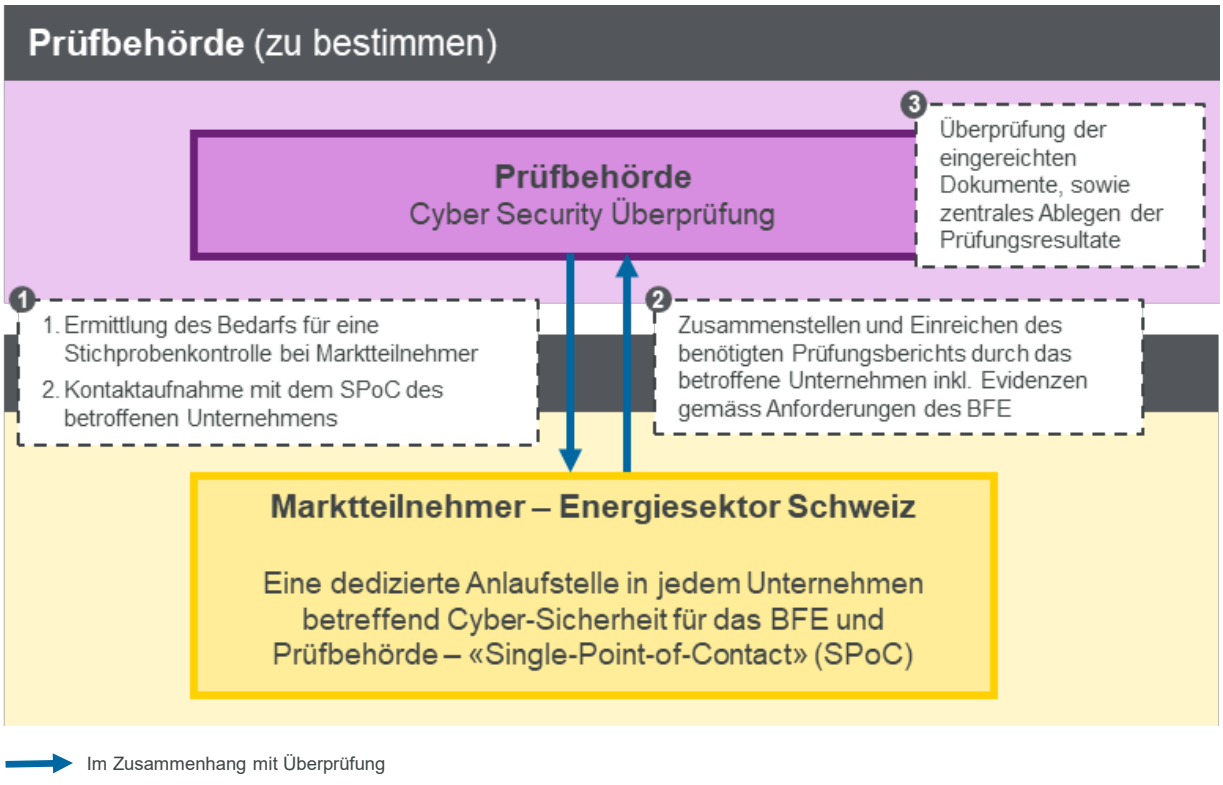


Abbildung 17: Stichprobenkontrollen

Stichprobenkontrollen wären ein weiteres, zentrales Instrument für die ordnungsgemässe Einrichtung und Ausübung der Überwachungs- und Überprüfungsfunktion der Prüfbehörde.

Im Gegensatz zu einer umfassenden Überprüfung (siehe Kapitel Audit) ginge es hierbei jedoch nicht um einen holistischen Nachweis der Konformität eines Marktteilnehmers mit bestehenden Cyber-Regulierungen. Vielmehr sollten Stichprobenkontrollen als ein komplementäres Instrument eingesetzt werden, um gewisse Aspekte gezielt bei einzelnen Marktteilnehmern überprüfen zu können.

Die Anwendung hierfür in der Praxis kann aus vielseitigen Aspekten für die Prüfbehörde von Interesse sein. Unter anderem könnten Stichprobenkontrollen die Umsetzung eines risikobasierten Ansatzes bei den Überprüfungstätigkeiten unterstützen und die Aufwände der Überprüfungstätigkeiten massiv reduzieren, ohne dabei jedoch auf Seiten der Prüfbehörde grössere Risiken eingehen zu müssen, so dass gröbere Gesetzesverstösse längerfristig nicht erkannt würden. Die wichtigsten Aspekte der gesetzlichen Anforderungen könnten gezielt etwas strenger bei den Marktteilnehmern kontrolliert werden und im Gegenzug dafür die Periodizität zwischen den jeweiligen, umfassenden Überprüfungstätigkeiten (siehe Kapitel Überprüfung / Audit) entsprechend ausgeweitet werden[76].

Auch könnten Stichprobenkontrollen durch die Prüfbehörde beispielsweise zur Anwendung kommen, um zeitnah zu überprüfen, ob korrigierende Massnahmen durch Marktteilnehmer umgesetzt wurden, welche während der letzten umfassenden Überprüfung für gewisse Bereiche als «nicht gänzlich gesetzes-konform» oder «verbesserungswürdig» eingestuft wurden. Ein anderes Anwendungsszenario könnte ebenfalls die Qualitätssicherung und konsistente Umsetzung der Überprüfungstätigkeiten sein, falls gewisse Überprüfungstätigkeiten externalisiert wurden. Die Prüfbehörde könnte parallel gewisse Stichprobenkontrollen durchführen, um zu kontrollieren, ob die eigenen Befunde deckungsgleich sind mit den angelieferten Resultaten der externen Dritten.

Würde der Bedarf für eine Stichprobenkontrolle bei einem Marktteilnehmer auch z.B. durch einen Zufallsprozess ermittelt, so sollte eine entsprechende Überprüfungsanfrage der Prüfbehörde analog der definierten Prozesse zur Anfrage für umfassende Überprüfungen geschehen. Gemäss den vorgeschlagenen Zielbild würde diese Art der Anfrage erneut mittels SPoC des betroffenen Marktteilnehmers intern koordiniert, welcher entsprechend die benötigten Evidenzen sammelt und fristgerecht an die Prüfbehörde übermittelt.

---

[76] *Bemerkung*: Die Eidgenössische Finanzmarktaufsicht (FINMA) hielt in ihrem Jahresbericht 2018 fest, dass sie verstärkt randomisierte Vor-Ort-Kontrollen mit Fokus auf die gestiegenen operationellen Risiken bei gewissen Institutionen durchführen wird. Es werden hierbei unter anderem Cyber-Risiken vermehrt berücksichtigt.

Selbstbeurteilungen

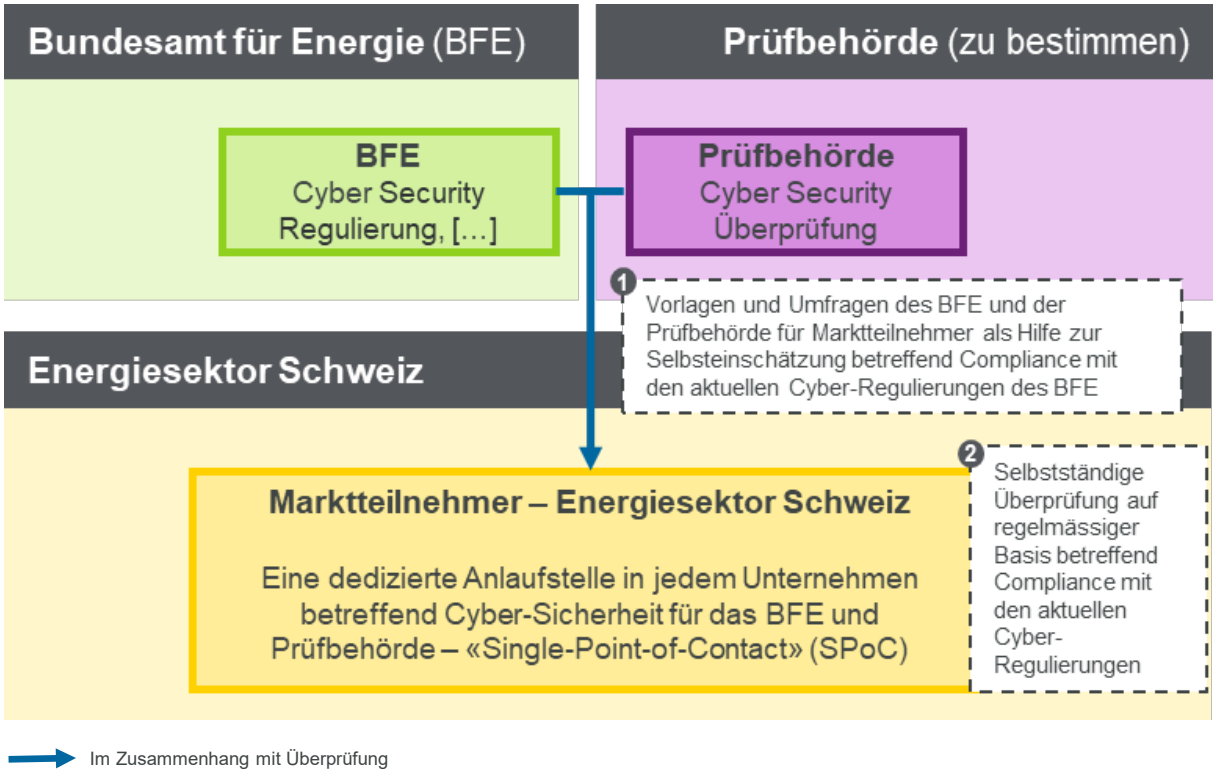


Abbildung 18: Selbstbeurteilungen

Institutionalisierte Anfragen und/oder Hilfestellungen zur Selbstbeurteilung könnten cyber-regulierten Unternehmen des Stromsektors Schweiz dabei helfen, selbstständig ihre Konformität mit den gesetzlichen Bestimmungen betreffend Cyber-Sicherheit und Resilienz laufend zu überprüfen. Auch kann dies dabei helfen, um sich besser auf künftige Überprüfungen oder Stichprobenkontrollen vorzubereiten.

Unverbindliche Hilfestellungen

Unverbindliche Hilfestellungen der Prüfbehörde und/oder des BFEs an die Marktteilnehmer könnten in unterschiedlicher Form erfolgen, so beispielsweise:

- Umfragen, wie in die durchgeführte «E-Survey» der vorliegenden Arbeit (siehe Kapitel 3),
- Self-Assessment Checklisten,
- weiterführende Implementierungsrichtlinien für gewisse Gesetzesanforderungen
- etc.

Diese auf Freiwilligkeit-basierenden Hilfestellungen würden eine erste Sensibilisierung der Unternehmen für gewisse Cyber-Thematiken ermöglichen und ihnen aktiv bei der initialen Umsetzung neuer Cyber- und Resilienz-Anforderungen helfen. Der Katalog der IKT-Minimalanforderungen des BWL, im Zusammenhang mit der E-Survey dieser Arbeit, ist ein gutes Beispiel bezüglich unverbindlicher Hilfestellungen (IKT-Minimalanforderungen) und einem Anreiz bzw. Aufruf zur Selbstbeurteilung (E-Survey).

Das Erstellen solcher neuen Hilfsmittel durch das BFE und/oder die Prüfbehörde sollte jedoch sehr gezielt und unter anderem auf Basis der gemachten Erfahrungen aus den Überprüfungstätigkeiten erfolgen und wenn immer möglich, auf bereits Bestehendes referenzieren (bereits bestehende Analogien und Weisungen des Bundes und der Kantone, internationale Standards, etc.).

Ein Bedarf für weitere Hilfsmittel könnte beispielsweise durch eine Zunahme von Anfragen betreffend die Umsetzung von Anforderungen, durch das Beobachten von Nichtkonformität gewisser Unternehmen oder aber auch durch die Tatsache einer Einführung gänzlich neuer Anforderungen jeweils abgeleitet werden.

Institutionalisierte Anfragen zur Selbstbeurteilung

Institutionalisierte Anfragen für eine verbindliche Teilnahme an einer Selbstbeurteilung bei den Betrieben durch die Prüfbehörde und/oder des BFE könnten als zusätzliches Instrument dabei helfen, gezielt eine Sensibilisierung und Bewusstsein («Awareness») für aktuelle Cyber-Gefahren und Themen bei den Marktteilnehmern zu erreichen [77]. Die relativ geringe Rücklaufquote der im Zusammenhang mit dieser Arbeit gemachten E-Survey könnte unter Umständen darauf hinweisen, dass eine gesetzlich verpflichtende Teilnahme benötigt wird, um diese Ziele zu erreichen.

Auch könnten Anfragen seitens des BFE und/oder der Prüfbehörde nach einzelnen Aspekten der Selbstbeurteilung eines Unternehmens beispielsweise dabei helfen, weiterführende Einblicke zu gewinnen, welche Bereiche wohl mit Priorität künftig stärker reguliert werden sollten, mehr Hilfestellungen zur erfolgreichen Implementierung geboten werden sollte oder mittels künftiger Stichprobenkontrollen vermehrt überprüft werden sollten. Um diese Zielsetzungen zu ermöglichen, müsste die verpflichtende Teilnahme der betroffenen Markteilnehmer an entsprechend deklarierten Selbstbeurteilungsanfragen von Seiten der Prüfbehörde und/oder des BFE erfolgen.

Auch unternehmensinterne Berichte betreffend Cyber-Gefahren und Risiken der Marktteilnehmer als Teil ihres Informationssicherheits-Managementsystems (ISMS), oder aber interne Compliance- und Revisionsberichte der Marktteilnehmer betreffend Cyber-Sicherheit und Resilienz könnten als eine Form der Selbstbeurteilung verstanden werden. Sie bilden eine gute Grundlage für die Beantwortung der bereits erwähnten institutionalisierten Anfragen zur Selbstbeurteilung (Umfragen). Entsprechend sollte evaluiert werden, ob die Prüfbehörde und/oder das BFE ebenfalls rechtlich verankerte Befugnis erlangen sollte, solche Dokumente entsprechend jederzeit anfordern zu können.

---

[77] *Bemerkung*: Die FINMA macht bereits von regelmässigen Selbstbeurteilungen bei grösseren Instituten brauch. Die regelmässige Selbstbeurteilung hilft die Unternehmen auf einen angemessenen Umgang mit Cyber-Risiken zu sensibilisieren und konzentriert sich auf die Fähigkeit der teilnehmenden Institute, die Cyber-Bedrohungslage im Hinblick auf institutsspezifische Verwundbarkeiten zu identifizieren, um darauf aufbauend eine Risikobeurteilung vorzunehmen und Massnahmen festzulegen. Für weiterführende Informationen: https://www.finma.ch/de/dokumentation/dossier/dossier-cyberrisiken/bedrohung-durch-cyber-attacken/

Zertifizierungen

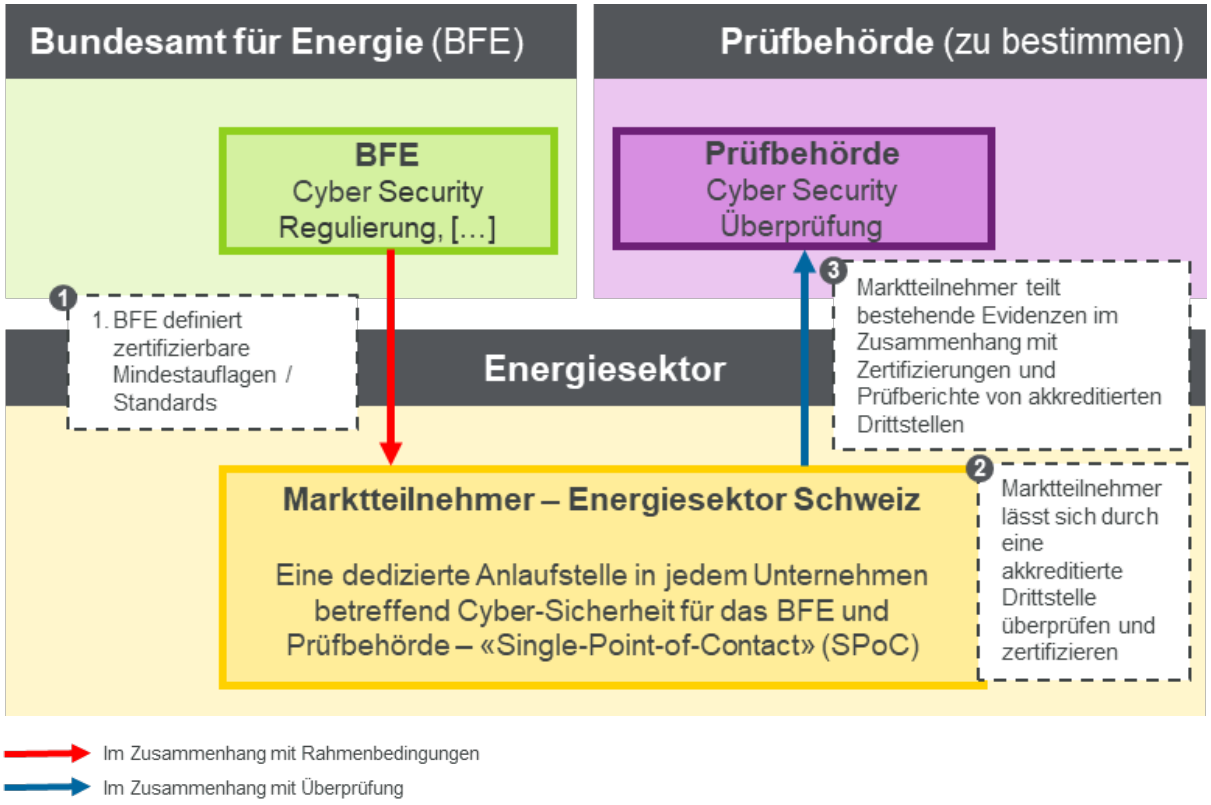


Abbildung 19: Zertifizierungen

Bei einer Zertifizierung handelt es sich um ein klar definiertes, standardisiertes Verfahren zum Nachweis der Einhaltung bestimmter Anforderungen durch Dritte (siehe auch ISO/IEC 17000, 5.5).

Akkreditierte Prüfstellen könnten engagiert werden, um die Konformität des zu Überprüfenden mit vordefinierten Anforderungen nachweisen zu lassen. Resultat dieser Tätigkeiten wäre ein Prüfbericht, sowie – bei einer erfolgreichen Überprüfung – die Ausstellung eines Zertifikates für den Überprüften, welches dessen Konformität bescheinigt.

Bei einer Akkreditierung handelt es sich um eine formale Bestätigung und Anerkennung der technischen Kompetenz der Prüfstelle (siehe auch ISO/IEC 1700, 5.6). Die Akkreditierung der Prüfstelle, sowie das standardisierte Prüfverfahren, würden ein einheitliches Qualitätsniveau der Überprüfungen sicherstellen. In der Schweiz wird diese Aufgabe durch die Schweizerische Akkreditierungsstelle (SAS) wahrgenommen, gestützt auf die Schweizerische Akkreditierungs- und Bezeichnungsverordnung (AkkBV).

Wird in der Schweiz gemäss NCS Massnahme 8 und Beschluss des Bundesrates auf Basis der Empfehlungen der Expertengruppe «Zukunft Datenschutz und Datensicherheit» ein verpflichtender Standard für den Schweizer Stromsektor definiert, welcher sich künftig durch externe Drittprüfstellen zertifizieren lässt, so würde dies die Externalisierung der Überprüfungsaufwände für die Prüfbehörde massiv vereinfachen. Marktteilnehmer des Schweizer Stromsektors könnten sich entsprechend durch unabhängige Drittstellen zertifizieren lassen und anschliessend die Resultate in der Form eines Prüfberichtes und einer Zertifizierung jeweils auf regelmässiger Basis der Prüfbehörde aushändigen.

Gewisse internationale Standards, wie beispielsweise die ISO Norm 27001 betreffend Informationssicherheits-Managementsystem (ISMS), sind global weit verbreitet und lassen sich bereits durch diverse akkreditierte Prüfstellen zertifizieren, so auch in der Schweiz. Auch einige Marktteilnehmer des Stromsektors Schweiz werden mit sehr hoher Wahrscheinlichkeit bereits diesen ISO Standard intern verfolgen und sind allenfalls sogar bereits entsprechend ISO 27001 zertifiziert[78]. Eine starke Anlehnung an internationale Standards, wie in Kapitel 4.1 entsprechend bereits ausgeführt, macht daher Sinn.

Nebst der vollständigen Akzeptanz bestehender, internationaler Standards bestünde alternativ auch die Möglichkeit, dass das BFE eine Abwandlung eines bereits bestehenden, internationalen Standards oder gar einen komplett eigens entwickelten Standard für Cyber-Sicherheit und Resilienz im Stromsektor Schweiz definiert. Auch in diesem Falle würde grundsätzlich die Option bestehen, dass dieser neu gezielt für den Schweizer Stromsektor spezifisch definierte Standard anschliessend gemeinsam mit Hilfe der SAS ebenfalls akkreditierbar gemacht wird [79].

Externe Drittprüfstellen könnten sich dann gemäss dem spezifisch für den Schweizer Stromsektor definierten Standard bei der SAS künftig akkreditieren lassen und anschliessend selbständig gemäss diesem Standard Markteilnehmer des Stromsektors Schweiz überprüfen und zertifizieren.

Offensichtlich wäre die Umsetzungsdauer dieser zweiten Variante jedoch wesentlich länger und es müsste sich zudem zuerst zeigen, ob genügend externe Drittprüfstellen gewillt wären, sich spezifisch nach diesem neuen, Schweizer Stromsektor-spezifischen Prüfstandard künftig bei der SAS akkreditieren zu lassen.

Die unten gezeigte Grafik veranschaulicht diese Variante nochmals:

Abbildung 20: Akkreditierungsprozess für externe Prüfstellen

78 Zum Beispiel zählt in Österreich die Energie- und Wasserversorgung als eine führende Branche mit ISO 27001 Zertifizierung mit rund 14% Beteiligung an den total ausgestellten Zertifizierungen, obwohl das österreichische Netz- und Informationssystemsicherheitsgesetz (NISG) diese Zertifizierung nicht explizit verlangt (Schuster 2021).

79 In Deutschland hat beispielsweise die Bundesnetzagentur in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik einen Sektor-spezifischen IT-Sicherheitskatalog veröffentlicht, nach welchem die Unternehmen sich bei einer akkreditierten Drittstelle zertifizieren lassen können. Die Anforderungen des IT-Sicherheitskatalog entsprechen grösstenteils ISO/IEC 27001 und ISO 27019. Die Zertifizierung wird als Nachweis für die Einhaltung der vorgegebenen Cyber-Anforderungen bei der Bundesnetzagentur eingereicht. Mehr Informationen hierzu in Anhang 5.

‚Incentives' / Sanktionierungen

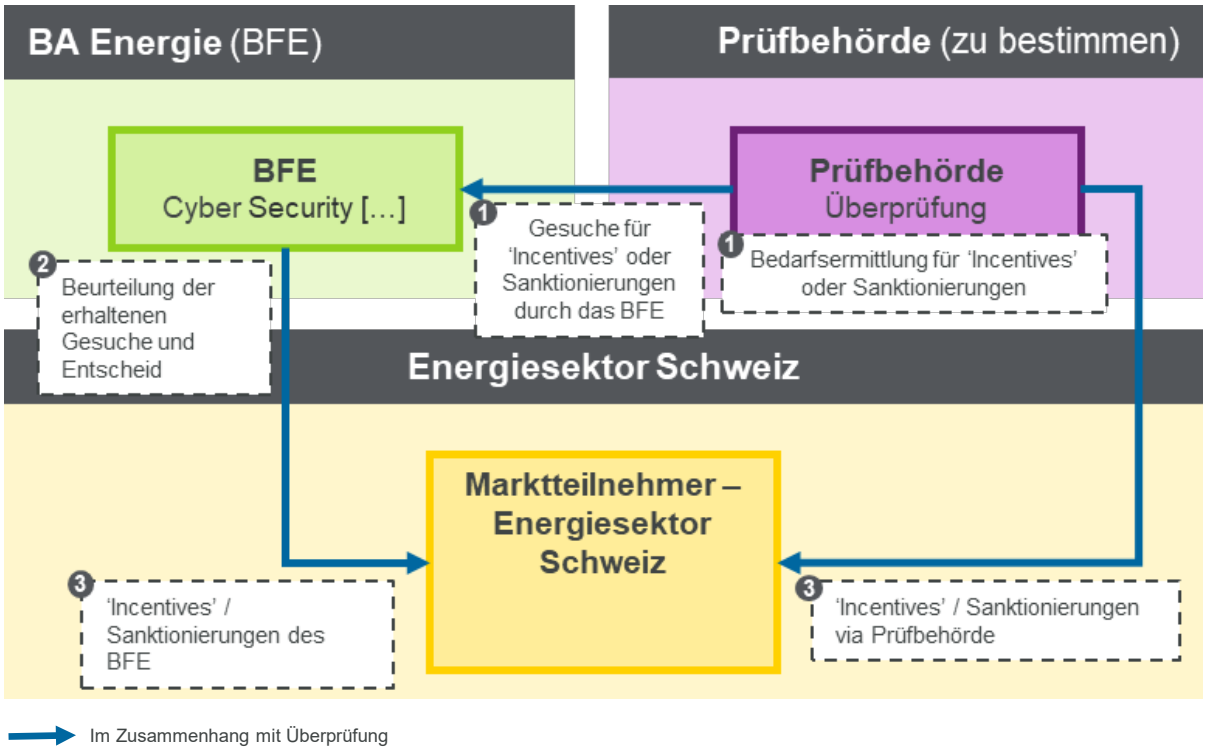


Abbildung 21: 'Incentives' / Sanktionierungen

Die Möglichkeiten der Sanktionierung und 'Incentivierung' wären weitere wichtige Instrumente für die Einrichtung der vorgeschlagenen Rahmenbedingungen.

Hat eine Nicht-Einhaltung gesetzlich verpflichtender Vorgaben keine negativen Konsequenzen, so ist der Anreiz diese Vorgaben auch entsprechend umzusetzen sehr gering. Dieser Umstand wird auch nicht durch verpflichtende Überprüfungen verbessert, diese decken eine Nicht-Konformität lediglich auf. Gewisse Sanktionierungsmöglichkeiten erscheinen daher als unumgänglich.

'Incentivierungen' sind im Gegenzug ein praktisches Steuerungsmittel zur Schaffung positiver Anreize. Sie könnten eingesetzt werden, um gewisse Massnahmen und Vorgaben zur Steigerung der Cyber-Sicherheit und Resilienz im Schweizer Stromsektor bereits umzusetzen, welche bis anhin noch nicht gesetzlich verankert wurden und als verpflichtend gelten. Es empfiehlt sich daher auch die entsprechenden Kompetenzen des BFE und/oder der Prüfbehörde im Bereich der Incentivierungs-Möglichkeiten zu ermöglichen.

In dieser Arbeit wird ein Sanktionierungs- / 'Incentivierungs'-Modell empfohlen, in welchem sowohl das BFE, als auch der Prüfbehörde gewisse Kompetenzen in diesen Bereichen zugesprochen würden.

Die Prüfbehörde sollte hierbei als überwachende und überprüfende Instanz bei der Aufdeckung einer gesetzlichen Nicht-Konformität eines Marktteilnehmers direkt selbst gewisse, kleinere Sanktionierungen sprechen können – analog dem Schweizerischen Ordnungsbussenverfahren im Strassenverkehr und den damit verbundenen Sanktionierungs-Kompetenzen der Polizei. Die Prüfbehörde sollte zudem auch die Kompetenzen erhalten, bei kleineren Verstössen jeweils nur Verwarnungen aussprechen zu dürfen.

Auch sollten der Prüfbehörde gewisse ‘Incentivierungs’-Kompetenzen zugesprochen werden, so dass sie künftig (teilweise) Anreize für eine Vereinfachung dessen Überprüfungsverfahrens schaffen kann. So wäre beispielweise vorstellbar, dass entstandene Kosten im Zusammenhang mit einer Zertifizierung gegenüber einem vom BFE und der Prüfbehörde akzeptierten Standard künftig übernommen oder weitergegeben werden dürfen. Für Marktteilnehmer, welche nicht Netzbetreiber sind und daher nicht die Möglichkeit haben ihre Kosten über die Tarife an Konsumenten weitergeben zu können, wäre unter Umständen eine Einführung direkter, zweckgebundener Unterstützungsleistungen zu prüfen. Auch ‘Incentivierungs’-Mechanismen im Sinne einer erleichterten Überprüfung, wie bspw. eine Reduktion der Wahrscheinlichkeit einer Stichprobenkontrolle zu unterliegen, wären denkbar.

Zugunsten des BFE sollten als regulierende Instanz im vorgeschlagenen Zielzustand entsprechend weitreichende Sanktionierungs- und ‘Incentivierungs’-Kompetenzen gesetzlich verankert sein. Das BFE würde somit gegenüber der Prüfbehörde deutlich grössere Sanktionierungen und ‘Incentivierungen’ aussprechen können. Entsprechend würde das BFE sich somit auf die gröberen Gesetzesverstösse fokussieren und die Prüfbehörde könnte bei Bedarf grösserer Sanktionierungen diese entsprechend beim BFE jeweils beantragen.

Während vorhergehend die Tätigkeiten, welche bei einer Sanktionierung und/oder ‘Incentivierung’ anfallen, besprochen wurde, zeigt der nachfolgende Abschnitt auf, welche Arten der Sanktionierung und/oder Anreize verwendet werden könnten. Nach einer kurzen Beschreibung der möglichen Instrumente, werden die Vor- (+) und Nachteile (-) in einer Aufzählliste aufgeführt.

Option 1: Sanktionierung

Eine Sanktion ist eine Massnahme, mit welcher man ein bestimmtes Verhalten erzwingen will oder mit der man ein bestimmtes Verhalten bestraft. Sanktionen in ihrer mildesten Variante könnten beispielsweise Verwarnungen sein. Weitere Möglichkeiten wären beispielsweise das Verhängen von Geldstrafen, der Entzug bereits bestehender Anreize (‘Incentivierungen’) oder im äussersten Fall sogar der Entzug der Betriebserlaubnis / ein Geschäftsverbot im Schweizer Markt sein [80].

+ Gängiges Mittel zur Durchsetzung von Vorgaben in der Schweiz, sowie in anderen Ländern
+ Effektives Werkzeug zur Durchsetzung der Einhaltung von Cyber-Regulationen im Energiesektor Schweiz
- Zusätzlicher Aufwand für die zuständigen Behörden, um sinnvolle Sanktionen zu identifizieren, sowie diese anschliessend jeweils in die Praxis umzusetzen.

Option 2: ‚Incentivierung‘

Eine ‚Incentivierung‘ ist eine Massnahme, welche geeignet sein soll, das Verhalten der Marktteilnehmer im Interesse des ‘Incentive’-Gebers mittels der Schaffung gezielter Anreize zu motivieren. ‘Incentivierungen’ können auf unterschiedlichste Weise ausgestaltet sein – ob finanzieller oder anderer Natur.

[80] In Deutschland und Frankreich werden beispielsweise Geldstrafen von bis zu 100‘000 EUR bei einer Nichteinhaltung der Sicherheitsanforderungen fällig.

Einige gängige Beispiele hierfür wären beispielsweise das Leisten von Direktzahlungen / Subventionen bei Erfüllung gewisser Kriterien oder das Schaffen zusätzlicher Verrechnungsmöglichkeiten vorhandener Kosten. Es wären aber auch völlig andere Formen denkbar wie beispielsweise:

- Weniger Kontrolle / Überprüfung bei Erbringen gewisser Nachweise, mehrjähriger Compliance, etc.
- Erbringen zentraler Dienstleistungen zur Gratis-Nutzung durch die Marktteilnehmer des Stromsektors Schweiz – bspw. ein zentrales Cyber-Trainingscenter zur Erbringung von Cyber-Trainings für Unternehmen, zentral organisierte Übungen, Gratis Threat Intelligence, etc.
- Das Versprechen, dass keine (neuen) verpflichtenden Vorgaben / neue regulatorischer Anforderungen vorzusehen oder Reportings in bestimmten Bereichen einzuführen oder zu verschärfen

Die folgenden Vor- und Nachteile wurden für die Incentivierung identifiziert:

+ Effektives Werkzeug zur Umsetzung weiterführender Anforderungen, welche über die aktuellen Cyber-Vorgaben des Energiesektors Schweiz hinausgehen und nicht verpflichtend sein sollen oder noch nicht geregelt sind

- Zusätzlicher Aufwand für die zuständigen Behörden, um sinnvolle ‚Incentivierungen' zu identifizieren, sowie diese anschliessend jeweils in die Praxis umzusetzen.

Option 3: Kombination Optionen 1 & 2

Die gemeinsame Nutzung gezielter Sanktionierungs-, als auch ‚Incentivierungs'-Massnahmen.

+ Alle oben genannten Vorteile der Optionen 1 & 2

- Alle oben genannten Nachteile der Optionen 1 & 2

Empfehlung Option 3
Kombination Sanktionierung und 'Incentivierung'

Option 3, also eine Kombination gezielter Sanktionierungs-, als auch ‚Incentivierungs'-Massnahmen, erscheint für die Schweiz als eine sinnvolle Variante, da so beide Instrumente je nach Bedarf und Angemessenheit gezielt eingesetzt werden könnten, womit die Durchsetzung der Cyber-Anforderungen in der Praxis gefördert würden.

Die zusätzliche Möglichkeit der 'Incentivierung' könnte beispielsweise auf dem bestehenden Modell aufgebaut werden, anhand dessen Netzbetreiber bereits heute Teile ihrer Cyber-Investitionen jeweils an ihre Endkunden weiterverrechnen dürfen. Ähnliche Anreize müssten entsprechend auch für andere Marktteilnehmer geschaffen werden, welche ihre Kosten aktuell nicht direkt an ihre Endkunden weiterverrechnen können.

Insbesondere ist auch zu prüfen, welche Erleichterungen im Überprüfungsprozess jeweils als 'Incentive' vorgesehen werden könnten. Dies könnte die künftigen Aufwände sowohl auf Seiten der Unternehmen, als auch bei der Prüfbehörde beträchtlich reduzieren.

4.3 Meldewesen

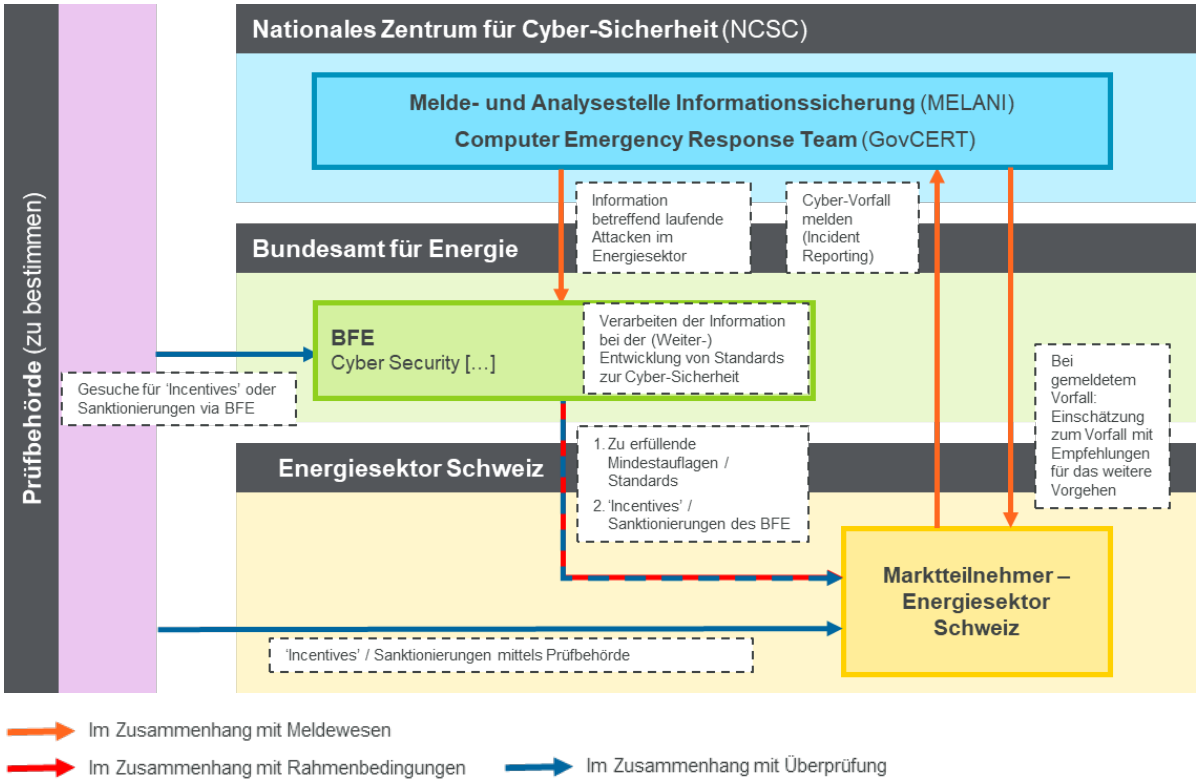


Abbildung 22: Meldewesen

Ein kontinuierlicher Wissensaustausch betreffend aktuell relevante Cyber-Gefahren und Risiken (Threat Intelligence), sowie das Meldewesen betreffend laufende Cyber-Attacken, sind zentrale Bestandteile eines gesamtheitlichen Cyber-Sicherheit und Resilienz Konzepts für den Schweizer Stromsektor. Die Einführung von Meldepflichten bei schwerwiegenden Sicherheitsvorfällen ist bereits ein vieldiskutiertes Thema und die Meinungen gehen dabei weit auseinander.

Aktuell wird das Thema Meldewesen innerhalb einer BFE Arbeitsgruppe erarbeitet, um die Etablierung, Ausgestaltung und zeitnahe Umsetzung einer Meldepflicht von Cyber-Vorfällen für die Unternehmen im Stromversorgungssektor Schweiz zu klären.

Denn in der Schweiz gibt es bis anhin keine sektorübergreifende, generelle Meldepflicht für Cyber-Vorfälle. Es besteht lediglich ein informeller, nicht Sektor-spezifischer Wissensaustausch zwischen gewissen Betreibern KI, welcher auf freiwilliger Basis via Melde- und Analysestelle Informationssicherung (MELANI) des Bundes organisiert wird.

Das aktive Melden von Cyber-Vorfällen durch die Marktteilnehmer, sowie das zentrale Überwachen aller laufenden Ereignisse erscheint jedoch als essentiell, damit a) das NCSC den betroffenen Unternehmen bei Bedarf helfen kann, den Cyber-Vorfall schneller zu überwinden, sowie b) das BFE die Möglichkeit hat, gewonnene Erkenntnisse in die künftige Weiterentwicklung der Cyber-Regulierungen mit einzubeziehen und/oder gezielte, neue 'Incentivierungen' und Hilfestellungen zeitgerecht unter Berücksichtigung aktueller digitaler Innovationen zu schaffen. Ohne eine solche Information bestünde die Gefahr,

dass die Regulierung den technischen Entwicklungen der Digitalisierung weit hinterherhinkt und nicht entsprechend reagiert und korrigiert werden kann.

Mit der zunehmenden Bedeutung von Cyber-Risiken, stellt sich zusätzlich die Frage, ob dieser bisher freiwillige, nicht institutionalisierte Wissensaustausch genügt, um künftig neue für den Schweizer Stromsektor relevante Cyber-Bedrohungen frühzeitig zu erkennen und sich entsprechend darauf vorbereiten zu können. Zudem besteht die Gefahr, dass die betroffenen Unternehmen bei einem freiwilligen, nicht institutionalisierten Wissensaustausch, und gleichzeitigen künftig eventuell «harten» Sanktionierungen bei Sicherheitsvorfällen die Risiken einer möglichen Sanktionierung bei Nicht-Meldung gegenüber der Sanktionierung der Meldung von Sicherheitsvorfällen gegeneinander abwägen würden.

Der Vergleich mit internationalen Erfahrungen auf Basis der NIS-Richtlinie in Kapitel 2 zeigte, dass in allen EU-Länder KI erhebliche Cyber-Sicherheitsvorfälle bei dafür dedizierten Stellen melden müssen. Im Rahmen der NCS wurde festgehalten, dass die Einführung von Meldepflichten bis spätestens Ende 2022 zu prüfen ist, wobei der Bundesrat Ende 2020 sich grundsätzlich für die Einführung von Meldepflichten für KI ausgesprochen hat.[81]

Analog hat das Parlament ein Postulat an den Bundesrat überwiesen, welches eine Ausarbeitung verlangt, wie Meldepflichten für Sicherheitsvorfälle bei KI künftig sektorübergreifend eingeführt werden können.[82] Ein erster Bericht zu möglichen Varianten für Meldepflichten von KI bei schwerwiegenden Sicherheitsvorfällen wurde vom Bundesrat 2019 veröffentlicht, welcher in die Erarbeitung der Meldepflicht für den Schweizer Strommarkt in dieser Arbeit mitberücksichtigt wurde.[83]

Für den Stromsektor wird, wie bereits erwähnt, derzeit innerhalb einer BFE Arbeitsgruppe an einer Sektor-spezifischen Meldepflicht gearbeitet, welche voraussichtlich im April 2021 definitiv verabschiedet wird. Wie in der nationalen Survey gezeigt wurde, befürwortet eine grosse Mehrheit der Umfrageteilnehmer (69%) eine Meldepflicht von Cyber-Sicherheitsvorfällen. Mit der Einführung eines institutionalisierten Meldewesens könnten unterschiedliche Ziele erreicht werden:

- Aufsichtspflicht des Staates gegenüber der Wirtschaft: Der Staat ist beauftragt nötigenfalls Massnahen zu ergreifen, falls gewisse Störungen das Funktionieren eines Sektors beeinträchtigen.
- Prävention vor Sicherheitsvorfällen: Unternehmen werden bei einer Einführung von Meldepflichten gezwungen, sich mit Sicherheitsvorfällen auseinanderzusetzen. Die internen Strukturen müssen somit angepasst werden, dass Vorfälle rechtzeitig erkannt und gemeldet werden können.
- Beurteilung der Bedrohungslage: Der risiko-basierte Regulierungsansatz kann mit einem zusätzlichen Informationsfluss besser auf die tatsächlichen Risiken reagieren und die Regulierung, falls nötig, flexibel anpassen.
- Frühwarnung durch Informationsaustausch: Analog zur Threat Intelligence, ist der Austausch über sicherheitsrelevante Vorfälle immer wichtiger aufgrund der zunehmenden Vernetzung und der steigenden Abhängigkeit zwischen den Unternehmen (z.B. Kaskadeneffekte). Die Meldepflichten ermöglichen, dass wichtige Informationen über mögliche Cyber-Attacken rasch zur Verfügung gestellt werden.

---

81 Bundesrat (2020), Medienmitteilung: Bundesrat spricht sich für eine Meldepflicht für kritische Infrastrukturen bei Cyberangriffen aus.

82 Postulat 17.3475 Graf-Litscher (2017), Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen.

83 Bundesrat (2019), Bericht: Varianten für Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen.

- Koordinierte Reaktion: Basierend auf der identifizierten Bedrohungslage, können konkrete Handlungsvorschläge abgegeben und gemeinsam abgestimmt werden.

Wahl der Meldestelle

Dieser Bericht legt zwei Optionen zur Wahl der künftigen Meldestelle von Cyber-Vorfällen im Schweizer Stromsektor vor. Nach einer kurzen Beschreibung der jeweiligen Option werden die entsprechenden Vor- (+) und Nachteile (-) aufgeführt.

Option 1: Zentrale, sektorübergreifende Meldestelle für relevante Cyber-Vorfälle

Diese Option beruht auf einer zentralen, sektorübergreifenden Meldestelle für relevante Cyber-Sicherheitsvorfälle.

+ Bestehende Strukturen des NCSC können genutzt werden, schnell operativ umsetzbar
+ Vorteile für die Erstellung eines gesamtheitlichen Cyber-Bedrohungslagebildes für alle kritischen Infrastrukturen, da Informationen der verschiedenen Sektoren zentral zusammenfliessen
+ Einfachere Koordination für die Bekämpfung sektorübergreifender Angriffe
- Weiterentwicklung der Cyber-Regulierung etwas schwieriger da die Regulierungsbehörde die Informationen noch indirekt über die Meldestelle erhalten

Option 2: Dezentrale Meldestelle für relevante Cyber-Vorfälle – spezifisch für den Schweizer Stromsektor

Diese Option beruht auf einer dezentralen, Sektor-spezifischen Meldestelle für relevante Cyber-Sicherheitsvorfälle im Stromsektor Schweiz.

+ Es bestehen bereits gewisse Meldepflichten und Meldemöglichkeiten bei schwerwiegenden Sicherheitsvorfällen im Stromsektor
- Sektorübergreifende Koordination ist nicht gewährleistet
- Bestehenden Meldestrukturen sind nicht auf die Meldung von Cyber-Vorfällen ausgerichtet. Die operative Einführung würde entsprechend eine längere Umsetzungsfrist benötigen

Empfehlung Option 1
Zentrale, sektorübergreifende Meldestelle

Dieser Bericht empfiehlt die bereits zentral vorhandenen Meldestrukturen des Bundes für den Schweizer Stromsektor zu nutzen (Option 1), da so alle Cyber-Vorfälle sektorübergreifend gesammelt und für die Threat Intelligence ausgewertet werden können. Zudem würde die Koordination bei einem grossflächigen Cyber-Angriff erheblich vereinfacht werden. Die Marktteilnehmer des Stromsektors

Schweiz würden somit künftig allfällige Cyber-Vorfälle dem NCSC melden, welches in engem Austausch mit dem BFE stehen würde.

Der Bundesratsentscheid für die Einführung der verbindlichen Meldepflicht bei KI, welcher nach der Erarbeitung dieser Empfehlung im Dezember 2020 veröffentlicht wurde, bestätigt die vorliegende Analyse und Empfehlung.

Bemerkung: Die eidgenössische Finanzmarktaufsicht (FINMA) fordert bereits seit Mai 2020 die finanzmarktaufsichtsrechtliche, obligatorische Meldepflicht bei wesentlichen Cyber-Attacken [84]. Die Aufsichtsmitteilung betrifft alle beaufsichtigten Institute und basiert auf Art. 29 Abs. 2 FINMAG. Um den Umfang der Meldepflicht einzugrenzen hat die FINMA ein Kriterienraster entwickelt, damit die betroffenen Institutionen den Schweregrad der jeweiligen Vorfälle selber ermitteln können [85]. Für die Schweregradeinstufung sind insbesondere die Dauer und das Ausmass der Beeinträchtigung in Bezug auf die Verfügbarkeit, Integrität und Vertraulichkeit der kritischen Aktiven (Daten, Technologiestruktur, Gebäude, Personal) massgeben.

Im Gegensatz zu der Empfehlung dieses Berichts für eine zentrale Variante der Meldepflicht im Schweizer Stromsektor, müssen die betroffenen Finanzinstitute im Gegensatz allfällige Vorfälle direkt an die FINMA melden. Die FINMA arbeitet entsprechend eng mit MELANI zusammen, um relevante Informationen betreffend Cyber-Vorfälle im Schweizer Finanzsektor sektorübergreifend verfügbar zu machen.

Umfang der Meldepflicht

Als «Umfang der Meldepflicht» wird einerseits der Adressatenkreis der Meldepflicht («*wer hat zu melden?*»), sowie die zu meldenden Inhalte verstanden («*was und ab wann ist zu melden?*»).

Bei der Frage zur Definition, welche Cyber-Vorfälle ab wann als «wesentlich» gelten und entsprechend zu melden sind, existieren in der Praxis grundsätzlich zwei Möglichkeiten. Entweder werden präzise Schwellenwerte definiert oder aber, die Definition wird bewusst offengelassen, um die Ausgestaltung möglichst flexibel zu halten. Die NIS-Richtlinie gibt hierzu die folgenden Aspekte exemplarisch vor, welche bei einer allfälligen Bestimmung von Schwellenwerten durch EU Mitgliedstaaten berücksichtigt werden sollten:

- Die Zahl der von der Unterbrechung der Erbringung des wesentlichen Dienstes betroffenen Nutzer;
- Die Dauer des Sicherheitsvorfalls; und
- Die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet.

---

84 «Das Kriterium der "Wesentlichkeit" ist erreicht, wenn der Schutz der Gläubiger, der Anleger und der Versicherten und/oder die Funktionsfähigkeit der Finanzmärkte beeinträchtigt wird. Das kann auch indirekt geschehen, z.B. bei Angriffen auf für die Institute kritische Infrastrukturen (ISPs, Stromerzeuger usw.). Im Fall einer Meldepflicht muss die Meldung "unverzüglich" erfolgen, d.h. durch Vororientierung der FINMA über den zuständigen (Key-)Account Manager innerhalb von 24 Stunden nach Feststellung der Cyber-Attacke und einer Erstbeurteilung über dessen Kritikalität, und durch die eigentliche Meldung innerhalb von 72 Stunden über die Erhebungs- und Gesuchsplattform (EHP) der FINMA.» (FINMA Aufsichtsmitteilung, 11.05.2020).

85 Eidgenössisches Finanzdepartement (2020) Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen - Rechtliche Grundlagen, S. 13.

Als weiterer, wichtiger Aspekt erscheint die prozedurale Ausgestaltung der Meldepflicht. So sollte beispielsweise festgelegt werden, in welchem Zeitraum die betroffenen Marktteilnehmer die Meldepflicht während Eintritt eines allfälligen Cyber-Vorfalls jeweils zu erfüllen haben und welche Sanktionen bei einer allfälligen Versäumnis drohen. Auch die Frage, ob und unter welchen Umständen anonyme Meldungen möglich sind, sollte entsprechend angedacht werden [86].

All die oben ausgeführten Aspekte wären bei der Einführung einer allfälligen Meldepflicht für den Schweizer Stromsektor ebenfalls idealerweise gesetzlich zu verankern, um die nötigen rechtlichen Grundlagen zu schaffen.

Die Sinnhaftigkeit solch einer Meldepflicht für Cyber-Sicherheitsvorfälle lässt sich insbesondere damit begründen, dass eine fehlende Versorgungssicherheit betreffend Strom auch direkte Folgen mit Auswirkungen auf Leib und Leben haben kann – beispielsweise bei fehlender Stromversorgung eines Spitals. Entsprechend dieser Begründung besteht ebenfalls analog bereits für Betriebsinhaber von Starkstromanlagen eine unverzügliche Meldepflicht an die zuständigen Kontrollstellen, für jede durch Elektrizität verursachte Personenschädigung oder erhebliche Sachbeschädigung (Art. 16 Abs.1 StromVG).

Schaffung von ‚Incentives' / Sanktionierungen zur Durchsetzung der Meldepflicht

Gemäss der bereits allgemein abgehandelten Thematik betreffend Möglichkeiten im Zusammenhang mit 'Incentives' und/oder Sanktionierungen (siehe Kapitel 4.1.2), setzt sich dieses Unterkapitel nun spezifisch mit möglichen Massnahmen im Zusammenhang mit der Durchsetzung einer allfälligen Meldepflicht auseinander.

Sanktionierung bei Versäumnis einer Meldepflicht und/oder nicht adäquatem Handeln

Die Versäumnis einer allfälligen Meldepflicht sollte rechtliche Konsequenzen haben, andernfalls besteht die Gefahr der Nichteinhaltung der Meldepflicht. Typischerweise geschieht dies in der Form von Geldstrafen.

Auch wäre zusätzlich ein Modell denkbar, bei welchem bei gemeldeten Cyber-Vorfällen jeweils im Nachgang im Sinne eines externen „Post-Incident Reviews" nochmals überprüft wird, ob der betroffene Marktteilnehmer auf den Cyber-Vorfall zum Zeitpunkt des Eintritts adäquat vorbereitet war und/oder ob der Marktteilnehmer während der Vorfalls-Bewältigung adäquat im Sinne des Regulators gehandelt hat – beispielsweise mit der obersten Priorität, kritische Infrastrukturen, sowie Leib und Leben zu schützen, anstelle der eigenen Finanzlage. Gefundene Missstände könnten entsprechend in resultierenden Sanktionen enden, so beispielsweise in der Form von Forderungen für eine schnelle Umsetzung von korrigierenden Massnahmen zur Stärkung der Cyber-Sicherheitslage des Marktteilnehmers.

+ Fördert dank abschreckender Wirkung möglicher Sanktionen die rasche und präzise Meldung von Cyber-Vorfällen durch betroffene Marktteilnehmer
+ Fördert dank abschreckender Wirkung möglicher Sanktionen die adäquate Vorbereitung auf Cyber-Vorfälle, sowie eine adäquate Vorfalls-Bewältigung im Sinne des Gesetzgebers
- Zusätzlicher Aufwand für zuständige Behörden, um sinnvolle Sanktionen jeweils zu identifizieren, sowie allenfalls zur Durchführung von „Post-Incident Reviews"

[86] In Anhang 5 zu den Praxisbeispielen Frankreich und Deutschland sind zwei konkrete Umsetzungsmöglichkeiten aufgeführt.

‚Incentivierung' zur Schaffung zusätzlicher Anreize, um Cyber-Vorfalle schnell und präzise zu melden

Bereits heute bietet der Bund zentral via NCSC und MELANI sektorübergreifend für alle Unternehmen der Schweiz gewisse Anreize an, welche zum Ziel haben die freiwillige Meldepflicht zu fördern. So beispielsweise direkte Hilfestellungen während der Bewältigung der Cyber-Krise der Betroffenen durch das GovCERT. Es können also zusätzliche Hilfestellungen von zentraler Seite her für betroffene Marktteilnehmer angeboten werden, um einen Cyber-Vorfall schneller und mit Erfolg zu bewältigen.

+ Die Attraktivität eine Meldung schnell und präzise abzugeben wird erhöht, dank dem zusätzlich geschaffenen Nutzen für Betroffene bei Bewältigung des Vorfalles
+ Die zusätzlichen, zentral gebotenen Hilfestellungen während der Vorfalls-Bewältigung erhöhen die Chancen auf eine schnelle und erfolgreiche Bewältigung der Ausnahmesituation durch die betroffenen Marktteilnehmer
- Zusätzlicher Aufwand für zuständige Behörden, um sinnvolle ‚Incentivierungen' jeweils zu identifizieren, sowie zusätzliche, zentrale Hilfestellungen während der Vorfalls-Bewältigung jeweils zur Verfügung zu stellen

Empfehlung betreffend Sanktionierung und 'Incentivierung'

Analog zu der Empfehlung betreffend Sanktionierung und 'Incentivierung' der Rahmenbedingungen und Überprüfung, wird betreffend der Thematik «Meldewesen» empfohlen, eine Kombination beider Instrumente einzusetzen, da diese so je nach Bedarf und Angemessenheit gezielt eingesetzt werden können.

Die 'Incentivierung' fördert eine schnelle und umfassende Bekämpfung allfälliger Cyber-Vorfälle, da die zuständige Behörde zielgerichtete Hilfestellungen dem betroffenen Unternehmen zur Verfügung stellen kann.

Die Wahl und Höhe einer Sanktionierung, typischerweise in der Form von Geldstrafen, sollte bei der Evaluierung den entsprechenden Risiken bei einer Nicht-Meldung gegenübergestellt werden.

4.4 Wissensaustausch

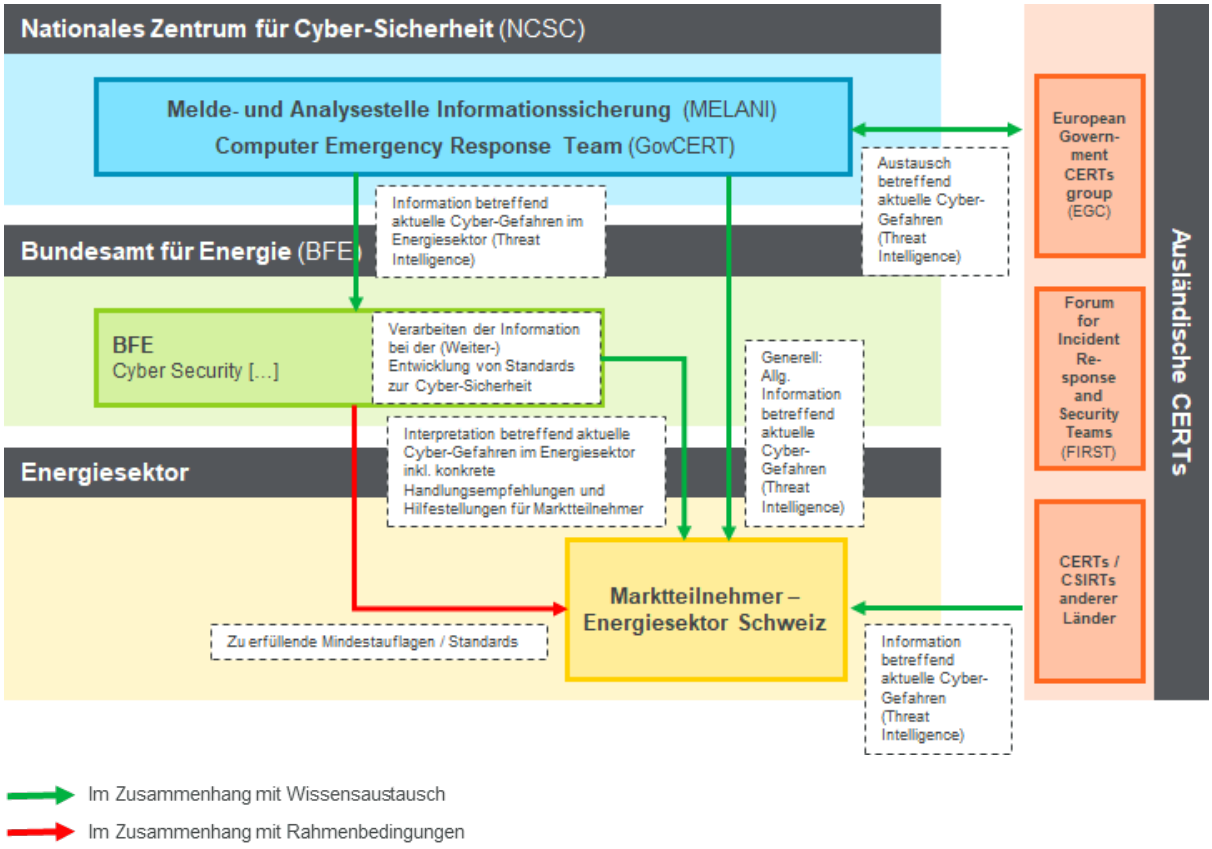


Abbildung 23: Wissensaustausch

Der kontinuierliche Wissensaustausch zu aktuellen Cyber-Gefahren (Threat Intelligence), ist ein wichtiges Instrument zur erfolgreichen Vermeidung und Abwehr von Cyber-Attacken. Innerhalb dieser Tätigkeit, werden die Bedrohungslage analysiert, sowie mögliche Angriffsszenarien ausformuliert. Basierend auf diesen laufenden Erkenntnissen und dem resultierenden Wissensvorsprung können sich die Marktteilnehmer gezielt gegen solche Angriffe wappnen.

Meldepflichten sind ein wesentlicher Bestandteil guter Threat Intelligence, da sie diese durch Teilen von Informationen betreffend reale Cyber-Vorfälle, sowie die damit verbundenen Praxiserfahrungen der Betroffenen, bereichern.

Der regelmässige, institutionalisierte Austausch über neueste Cyber-Entwicklungen, Cyber-Risiken auch insbesondere im Zusammenhang mit Digitalisierung, die aktuelle Cyber-Bedrohungslage, sowie über vergangene Cyber-Vorfälle, erscheinen als wichtig, damit sich die Marktteilnehmer des Schweizer Stromsektors gezielt künftig präventive Schutzmassnahmen ergreifen können.

Betreffend kritische Infrastrukturen (KI) haben viele Staaten in der Zwischenzeit ebenfalls sektorübergreifende Plattformen geschaffen und fördern diesen Informationsaustausch speziell zwischen KI-Betreibern aktiv. Auch der Schweizer Bundesrat hat erkannt, dass ein sektorübergreifender Informationsaustausch ein Schlüsselelement zum Schutz vor grossflächigen KI-Ausfällen ist. In der Schweiz fördert und betreibt der Bund daher seit dem Jahr 2004 mittels MELANI solch einen entsprechenden, institutionalisierten Wissensaustausch, welcher sektorübergreifend betrieben wird.

Cyber-Vorfälle können sich zudem durch die starke globale Vernetzung und die entsprechenden Abhängigkeiten schnell und unabhängig von nationalen Grenzen verbreiten. Eine internationale, wirksame und vertrauensvolle Kooperation betreffend Cyber-Gefahren ist daher essentiell. Dem NCSC kommt beim institutionalisierten Wissensaustausch sowohl in der Schweiz, als auch über die Landesgrenzen hinweg eine zentrale Rolle zu. So betreibt das NCSC selbst das Government Computer Emergency Response Team (GovCERT) des Bundes, welches regelmässig im engen Austausch betreffend laufende Cyber-Attacken mit anderen internationalen CERTs steht. Das NCSC sammelt und verteilt erhaltene «Threat Intelligence» Informationen hierbei nicht nur, sondern analysiert und bereitet diese auch gemäss NCS Massnahme 4 «Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage» regelmässig in Berichtsform auf.

Es wird an dieser Stelle zusätzlich vorgeschlagen, dass die bereits heute durch das NCSC regelmässig erstellten «Threat Intelligence» auch vom BFE und der Prüfbehörde künftig ihre Verwendung finden sollten, um die Aufsichts- und Überprüfungstätigkeiten künftig laufend vor dem Hintergrund der neueste Cyber-Innovationen weiter zu entwickeln und Sektor-spezifische Cyber-Regulierungen entsprechend der jeweils aktuellen Cyber-Bedrohungslage für den Stromsektor Schweiz entsprechend anzupassen. Momentan fokussieren sich die öffentlich zugänglichen Informationen auf «Top Cyber-Bedrohungen des aktuellen Monats», was aber gemäss NCS 2018-2022 weiter ausgebaut werden soll. Dazu braucht es eine systematische Nutzung von Open Source Intelligence (OSINT) und den damit verbundenen Fachkenntnissen, die Nutzung technischer Hilfsmittel sowie die Pflege und der Ausbau des Netzwerkes an nationalen und internationalen Partnern. Die gewonnenen Erkenntnisse zur Bedrohungslage sind systematisch aufzuarbeiten, regelmässig zu aktualisieren und über den Lageradar zielgruppengerecht darzustellen. Es soll auch eine Version des Lageradars für die Öffentlichkeit erstellt werden. Schliesslich sind dazu sind seitens Fachamt die entsprechenden Strukturen aufzubauen.

Dies würde ebenfalls bedeuten, dass auch BFE und Prüfbehörde künftig einen Teil der Sektor-spezifischen Aufbereitungsarbeiten von «Threat Intelligence» Informationen übernehmen sollten. Dadurch könnten das Fachamt und die Prüfbehörde die Marktteilnehmer des Stromsektors Schweiz entsprechend auch zusätzlich auf Sektor-spezifische, grössere Bedrohungen und relevante Lageveränderungen sensibilisieren, sowie zusätzliche Empfehlungen und Hilfestellungen zur Prävention gegen mögliche Cyber-Attacken innerhalb des Sektors abgeben.

4.5 Zusammenfassung

Abschliessend werden all die in diesem Kapitel jeweils vorgeschlagenen Optionen nochmals mittels zwei übergreifender Darstellungen visualisiert, um das Zusammenspiel der verschiedenen Handlungsfelder besser aufzeigen zu können.

Zunächst zeigt Abbildung 24 die Dynamik zwischen den Feldern «Rahmenbedingungen» und «Überprüfung». Abbildung 25 fokussiert sich anschliessend auf das Zusammenspiel der Handlungsfelder «Meldewesen» und «Wissensaustausch».

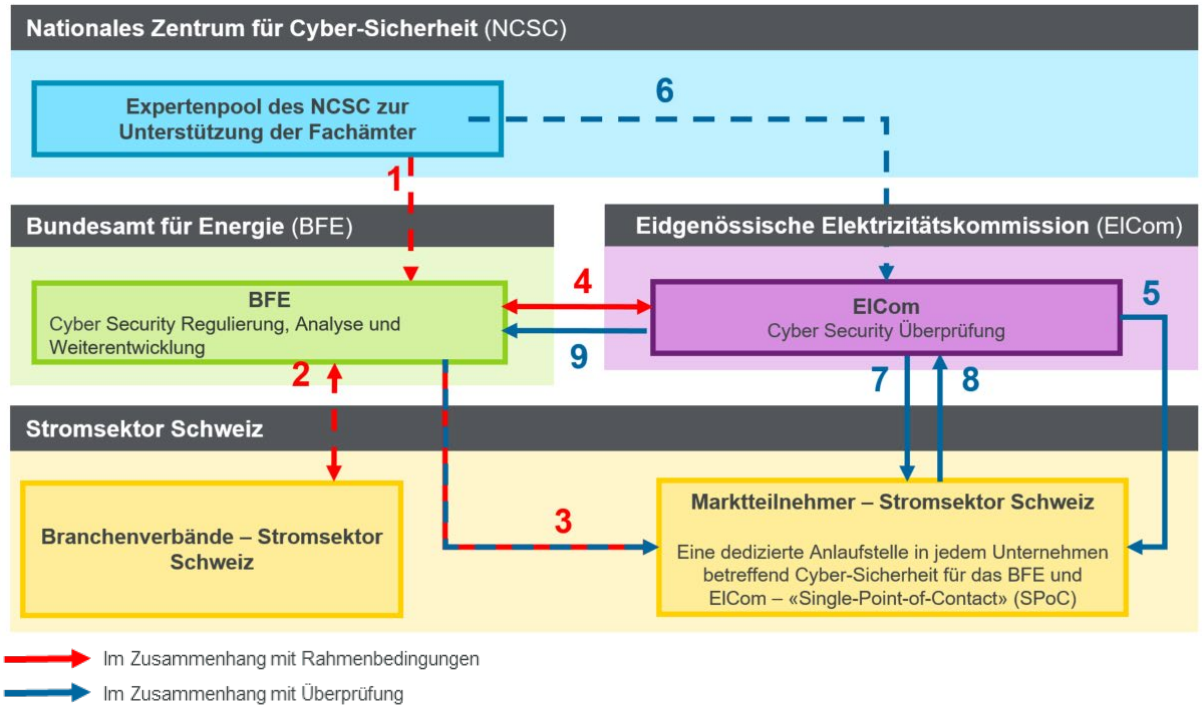


Abbildung 24: Zusammenspiel der Handlungsfelder «Rahmenbedingungen» und «Überprüfung»

Tabelle 10: Zusammenspiel der Handlungsfelder «Rahmenbedingungen» und «Überprüfung»

#	Beschreibung
1	Auf Anfrage des BFE: Unterstützung bei der Entwicklung von Standards zur Cyber-Sicherheit
2	Informeller Austausch betreffend verpflichtende Mindestauflagen und entsprechende, technische Standards
3	1. Zu erfüllende Mindestauflagen / Standards 2. ‘Incentives’ / Sanktionierungen des BFE
4	Regelmässiger Austausch betreffend zu überwachende Mindestauflagen / Standards und Stand der Umsetzung aller Marktteilnehmer
5	‘Incentives’ / Sanktionierungen durch die Prüfbehörde
6	Auf Anfrage der Prüfbehörde: Unterstützung bei der Überprüfung und praktischen Umsetzung von Standards zur Cyber-Sicherheit
7	1. Informationsanfragen und Kontrollen im Rahmen von Stichproben 2. Periodische Überprüfungen (Audits)
8	1. Zertifizierungen 2. Externe Prüfungsberichte und Evidenzen 3. Interne Prüfungsberichte und Self-Assessments
9	Gesuche für allfällige ‘Incentives’ oder Sanktionierungen durch das BFE

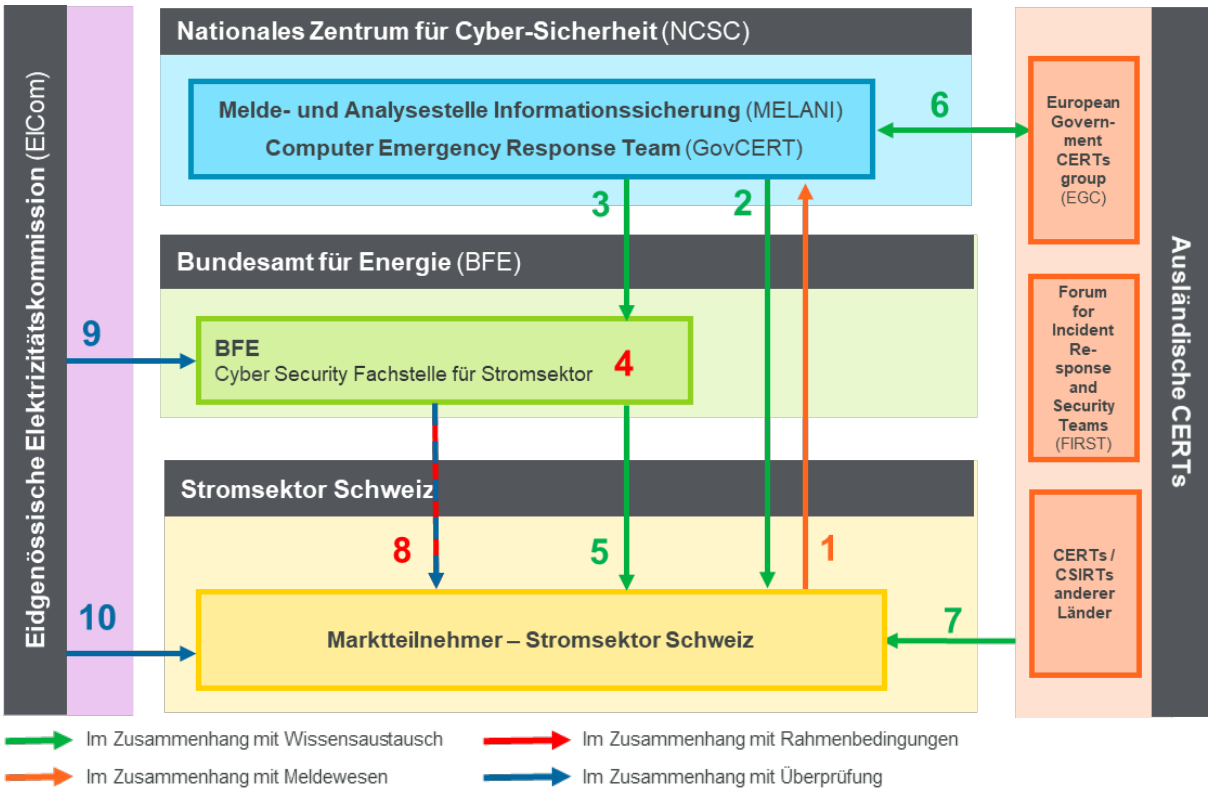


Abbildung 25: Zusammenspiel der Handlungsfelder «Wissensaustausch» und «Meldewesen»

Tabelle 11: Zusammenspiel der Handlungsfelder «Wissensaustausch» und «Meldewesen»

#	Beschreibung
1	Meldung von Cyber-Vorfall (Incident Reporting)
2	Interpretation betreffend aktuelle Cyber-Gefahren (Threat Intelligence) inkl. konkrete Handlungsempfehlungen und Hilfestellungen bei Meldung von Cyber-Vorfällen für Marktteilnehmer
3	Information betreffend aktuelle Cyber-Gefahren und laufenden Attacken im Stromsektor (Threat Intelligence)
4	Verarbeiten der Information bei der (Weiter-) Entwicklung von Mindestanforderungen zur Cyber-Sicherheit
5	Interpretation betreffend aktuelle Cyber-Gefahren im Energiesektor (Threat Intelligence) inkl. sektorspezifische Handlungsempfehlungen und Hilfestellungen für Marktteilnehmer
6	Austausch betreffend aktuelle Cyber-Gefahren (Threat Intelligence)
7	Information betreffend aktuelle Cyber-Gefahren (Threat Intelligence)
8	1. Zu erfüllende Mindestauflagen / Standards 2. ‘Incentives’ / Sanktionierungen des BFE
9	Gesuche für Sanktionierung von Prüfbehörde bei Feststellung von nicht gemeldeten, schwerwiegenden Cyber-Vorfällen im Rahmen der umfassenden Überprüfung der Sicherheits-anforderungen
10	‘Incentives’ / Sanktionierungen mittels Prüfbehörde

Fazit Kapitel 4 – Vorgeschlagene Optionen zur Adressierung des Handlungsbedarfs

Entlang der in den Kapitel 3 identifizierten vier Handlungsfelder wurde innerhalb dieses Kapitels ein initiales Konzept zur künftigen Umsetzung von Cyber-Sicherheit und Resilienz im Schweizer Stromsektor erarbeitet, welches mögliche Handlungsoptionen und Massnahmen zur künftigen Stärkung des Sektors im Cyber-Bereich transparent aufzeigt, sowie konkrete Handlungsempfehlungen abgibt.

Die Institutionalisierung von Rahmenbedingungen inklusive dem Schaffen gesetzlich verpflichtender Mindest-Anforderungen betreffend Cyber-Sicherheit und Resilienz innerhalb des Stromsektors Schweiz erscheint als unumgänglich. Das BFE als Fachamt in den Bereichen Risikomanagement, Regulierung und Digitalisierung scheint prädestiniert dafür, diese Aufgaben künftig innerhalb des Schweizer Stromsektors wahrzunehmen (siehe auch Kapitel 4.1).

Um eine erfolgreiche Umsetzung allfälliger Cyber- und Resilienz-Anforderungen innerhalb des Stromsektors Schweiz sicherstellen zu können, erscheint es als notwendig, künftig entsprechend eine zusätzliche Prüfbehörde zu etablieren, welche die Einhaltung solcher Anforderungen innerhalb des Sektors überwacht. Mehrere Optionen betreffend mögliche Instrumente und Mechanismen zur Überprüfung und Durchsetzung neuer Anforderungen wurden hierbei in diesem Kapitel vorgestellt, welche künftig idealerweise alle in Kombination ihre Anwendung finden sollten (siehe auch Kapitel 4.2).

Des Weiteren erscheint die Einführung einer gesetzlich verankerten Meldepflicht für wesentliche Cyber-Vorfälle im Schweizer Stromsektor künftig als unumgänglich. Eine entsprechende Ausgestaltung ist an den Bundesratsentscheid von Ende 2020 geknüpft und künftig dem voraussichtlich im April 2021 Sektor-spezifischen Vorschlag und Entscheid anzugleichen (siehe auch Kapitel 4.3).

Als Teil der Aktivitäten im Bereich des Wissensaustauschs («Threat Intelligence») würden künftig idealerweise direkt konkrete, für den Stromsektor massgeschneiderte Hilfsstellungen regelmässig an alle Marktteilnehmer verteilt, welche ihnen jeweils dabei helfen, sich situativ jeweils auf die aktuelle Cyber-Gefahrenlandschaft besser vorzubereiten (siehe auch Kapitel 4.4).

5 Umsetzungsplan der vorgeschlagenen Optionen

Die vorgeschlagenen Optionen zur Umsetzung des identifizierten Handlungsbedarfs umfassen eine Reihe von Möglichkeiten, welche den vorherig identifizierten Handlungsbedarf betreffend Cyber-Sicherheit und Resilienz im Stromsektor Schweiz angehen. In diesem Kapitel wird versucht, die benötigten Schritte zusammenzufassen und eine mögliche zeitliche Abfolge aufzuzeigen.

In den untenstehenden Tabellen werden links die präsentierten Optionen des Kapitel 4 aufgelistet. In der rechten Spalte werden die Schritte (= S), welche bei der Umsetzung des jeweiligen Vorschlags zu erreichen sind, aufgeführt.

Zudem wird ausgewertet wie die vorgeschlagene Option jeweils dazu beitragen könnte gewisse referenzierte Massnahmen (= M) der NCS 2018-2022 umzusetzen.

Es wird auch eine Angabe zu der etwaigen Zeitspanne (K = kurzfristig, L = langfristig) des vorgeschlagenen Schritts angegeben. Die kurzfristigen Schritte sollten bis Ende 2022 eingesetzt werden, damit die Massnahmen der NCS 2018-2022 zeitgemäss erfüllt werden können; langfristige Schritte sollten nach 2022 ausgeführt werden. Gantt-Diagramme zeigen diese zeitliche Abfolge visuell auf.

Da die Vorschläge sehr weitreichend sind, werden die Schritte auch in «zwingend» (# in Orange und -Ikon) und «optional» (# in Gelb und -Ikon) aufgeteilt.

Letztlich, wird für jeden Schritt auch der ungefähre Aufwand von den relevanten Akteuren für deren Umsetzung geschätzt. Diese Angaben sind relativ zu verstehen und sollten mit Vorsicht betrachtet werden. Es ist anzumerken, dass dies keine Kostenschätzung reflektiert, da diese sehr stark von der Ausarbeitung der Elemente abhängt ist und dieser Bericht primär darauf abzielt, Diskussionsgrundlagen vorzuschlagen.

Tabelle 12 zeigt die grundlegenden Schritte, welche für die Ernennung der zuständigen Behörden benötigt sind, auf. Die Tabellen 14, 16 und 18 benennen die möglichen Schritte zur Erreichung der vorgeschlagenen Optionen entlang den vier Bereichen der Rahmenbedingungen, der Überprüfung, des Meldewesens und des Wissensaustauschs.

Die untenstehende Tabelle zeigt zwei grundlegende Schritte auf, welche zur Ernennung von national zuständigen Behörden für den Schweizer Stromsektor betreffend Cyber-Sicherheit und Resilienz benötigt würden. Dies betrifft primär die Schaffung von den gesetzlichen Mandaten, damit die anderen Bereiche umgesetzt werden können.

Tabelle 12: Umsetzung der vorgeschlagenen Optionen - Grundlegende Schritte

#	Vorgeschlagene Option	NCS	Zeit-spanne	Auf-wand	Schritte zur Erreichung der Option
1	Die **Zuständigkeiten** im Bereich Cyber zwischen BFE und der Prüfbehörde sind geklärt und die **Grundlagen** für die Bezeichnung sowie Zuweisung der Mandate sind geschaffen. Das BFE als Fachamt für Cyber-Sicherheit im Stromsektor entwickelt den regulatorischen Rahmen. Die Einhaltung des regulatorischen Rahmens wird durch die zu bestimmende Prüfbehörde sichergestellt.	NCS Allg.	K		**S01.1** Die Rollen und Verantwortlichkeiten des BFE und der Prüfbehörde sind basierend auf den Vorschlägen geschärft gegeneinander abgegrenzt.
			K - L		**S01.2** Die rechtlichen Grundlagen sind präzisiert und/oder werden geschaffen, damit die Mandate gesetzlich abgesichert sind.
2	Die **Zusammenarbeit zwischen dem BFE und dem NCSC** ist institutionalisiert.	NCS Allg.	K		**S02.1** Eine enge Kooperation mit klar geregelten und ggf. regulatorisch verankerten Aufgaben zwischen NCSC, dem BFE, der Prüfbehörde und anderen Instanzen ist nachhaltig aufgestellt.

Tabelle 13: Gantt-Diagramm - Grundlegende Schritte

#	Bis Ende 2022 (K)	Nach 2022 (L)
S01.1 Abgrenzung von Rollen & Verantwortlichkeiten im Bereich Cyber		
S01.2 Institutionalisierung von rechtlichen Grundlagen für Mandate		
S02.1 Regelung NCSC Zusammenarbeit		

5.1 Rahmenbedingungen

Die untenstehende Tabelle zeigt die nötigen Schritte zur Erreichung der vorgeschlagenen Optionen für den Bereich der Rahmenbedingungen gemäss Kapitel 4.1 auf.

Tabelle 14: Umsetzung der vorgeschlagenen Optionen - Rahmenbedingungen

#	Vorgeschlagene Option	NCS	Zeit-spanne	Auf-wand	Schritte zur Erreichung der Option
3	Verpflichtende **Cyber-Anforderungen** für relevante Marktteilnehmer sind identifiziert und verankert. Die Anforderungen folgen einem risikobasierten Regulierungsansatz. Strukturen und Prozesse werden etabliert, um die Cyber-Anforderungen den Entwicklungen der Digitalisierung anzupassen. Weiter sind die Anforderungen für die relevanten Marktteilnehmer selektiv auf Basis von bestehenden nationalen Grundlagen und internationalen Frameworks und Standards erarbeitet.	M8	K	▂▄▆	**S03.1** Die Cyber-Anforderungen sind identifiziert. Es wurden hierfür drei untergeordnete Schritte unternommen: 3. Es ist sichergestellt, dass ein gewisser Cyber-Grundschutz für relevante Marktteilnehmer im Schweizer Stromsektor gegeben ist. 4. Inhaltliche Harmonisierung und Abgleich mit dem verpflichtenden Grundschutz sowie Weiterentwicklung der cyber-relevanten, zusätzlichen Anforderungen für Betreiber kritischer Infrastrukturen innerhalb des Stromsektors Schweiz. 5. Sind diese beiden Kategorien zufriedenstellend aufeinander abgestimmt, so empfiehlt es sich weiterführenden, Stromsektor-spezifischen Anforderungen zu widmen, welche über den gewünschten Grundschutz herausgehen.
			L	▂▁▁	**S03.2** Die erarbeiteten Cyber-Anforderungen sind verbindlich für die jeweils betroffenen Marktteilnehmer in Kraft getreten.
			L	▂▄▁	**S03.3** Die Anforderungen werden dynamisch weiterentwickelt, wobei sie an mögliche, relevante Veränderungen in der Cyber-Bedrohungslandschaft angepasst werden.

Tabelle 15: Gantt-Diagramm - Rahmenbedingungen

#	Bis Ende 2022 (K)	Nach 2022 (L)
S03.1 Identifizierung von Cyber-Anforderungen	▬▬▬▬▬▬	
S03.2 Cyber-Anforderungen treten in Kraft		▬
S03.3 Weiterentwicklung Cyber-Anforderungen		▬▬▬▬▬▬

5.2 Überprüfung

Für den Bereich der Überprüfung gemäss Kapitel 4.2 wären gemäss den präsentierten Optionen die folgenden Schritte relevant.

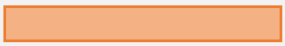
Tabelle 16: Umsetzung der vorgeschlagenen Optionen - Überprüfung

#	Vorgeschlagene Option	NCS	Zeit-spanne	Auf-wand	Schritte zur Erreichung der Option
4	Der **Registrierungsprozess** und ein **Register** zur Umsetzung der Regulierungsvorgaben und effizienten Marktkommunikation sind eingerichtet. Dies beinhaltet die vollständige Registrierung der relevanten SPOCs.	M8	K	▂▄▯	**S04.1** Die Ausgestaltung des Registrierungsprozesses und des Registers ist klar. Die notwendigen rechtlichen Grundlagen für eine verpflichtende Registrierung der Unternehmen sind identifiziert. Eine freiwillige Registrierung der Unternehmen hat so möglich begonnen.
			L	▂▯▯	**S04.2** Die neue Regelung tritt in Kraft und die relevanten Marktteilnehmer sind verpflichtet sich bei der Prüfbehörde zu registrieren. Ebenso ist die Befugnis zum Informationszugang BFE rechtlich festgelegt.
			L	▂▯▯	**S04.3** Alle relevanten Marktteilnehmer sind bei der Prüfbehörde registriert. Der Informationsfluss mit den nötigten Informationen für das Register ist nachhaltig sichergestellt.
5	Die Prüfbehörde führt auf regelmässiger Basis bei ausgewählten Marktakteuren **umfassende Überprüfungen** (Audits) durch, um die Einhaltung der Cyber-Anforderungen bei allen relevanten Unternehmen sicherzustellen.	M8	K	▂▄▉	**S05.1** Die notwendigen, rechtlichen Befugnisse der zuständigen Prüfbehörde sind für dieses Handlungsfeld geprüft. Notwendige zusätzliche gesetzliche Grundlagen sind identifiziert und werden erarbeitet. Die detaillierte Ausgestaltung des Prüfprozesses inklusive Stichprobenkontrollen und Selbstbeurteilungen ist klar.
			L	▂▯▯	**S05.2** Die neue Regelung, welche die umfassende Überprüfung der Cyber-Anforderungen durch die Prüfbehörde ermöglicht, erreicht Gültigkeit.
			L	▂▄▯	**S05.3** Die Prüfbehörde hat die benötigten Prozesse und Systeme für die Überprüfungstätigkeiten eingesetzt und führt regelmässig Überprüfungen bei allen relevanten Unternehmen durch.

#	Vorgeschlagene Option	NCS	Zeit-spanne	Auf-wand	Schritte zur Erreichung der Option
6	Die Prüfbehörde führt in gewissen, periodischen Intervallen **Stichproben-kontrollen** bei den Betrieben als komplementäres Instrument zu der umfassenden Überprüfung durch, um gewisse Aspekte gezielt und nachhaltig bei einzelnen Marktteilnehmern zu überprüfen.	M8	K	▂▄▁	**S06.1** Die rechtliche Befugnis, dies als Teil des Prüfmandats umsetzen zu können, ist abgeklärt und wird so nötig geschaffen.
			L	▂▁▁	**S06.2** Die neue gesetzliche Regelung tritt in Kraft.
			L	▂▁▁	**S06.3** Die Art und Weise (z.B. Inhalte oder Regelmässigkeit) der Stichproben wird laufend überarbeitet. Die Prüfbehörde verfügt über die nötigen Kontrollfähigkeiten und führt in gewissen, periodischen Intervallen Stichprobenkontrollen durch.
7	Die Unternehmen führen freiwillige und institutionalisierte **Selbstbeurteilungen** durch. Die Prüfbehörde und das BFE können diese Beurteilungen teils einfordern, um die Cyber-Anforderungen ggf. anzupassen.	M8	K	▂▄▁	**S07.1** Standardisierte Umfragen zur Selbstbeurteilung sind erarbeitet. Eine Verpflichtung zur Teilnahme an Umfragen ist Kraft oder vorgesehen.
			K	▂▁▁	**S07.2** Das Teilen von nicht-anonymisierten Selbstbeurteilungen mit der Prüfbehörde und/oder BFE ist geprüft und wird ggf. verankert.
			L	▂▁▁	**S07.3** Die neue gesetzliche Regelung tritt in Kraft.
			L	▂▄▁	**S07.4** Die freiwilligen und institutionalisierten Selbstbeurteilungen werden von den Betrieben durchgeführt und wo festgelegt mit dem BFE und/oder der Prüfbehörde geteilt. Die eingereichten Beurteilungen werden fortwährend von dem BFE genutzt, um die Cyber-Anforderungen weiterzuentwickeln.

#	Vorgeschlagene Option	NCS	Zeit-spanne	Auf-wand	Schritte zur Erreichung der Option
8	**Zertifizierungen** werden als Nachweis der Einhaltung bestimmter Anforderungen im Rahmen der regelmässigen Überprüfung bei der Prüfbehörde anerkannt.	M8	K	▂▄▁	**S08.1** Es ist abgeklärt, wie akkreditierte Prüfstellen die Konformität des zu Überprüfenden mit den Cyber-Anforderungen für die Prüfbehörde nachweisen können. Die Auslegung dieses Elements ist stark von den Bestimmungen der Regulierung «S03.1 Cyber-Anforderungen» abhängig. Entweder können bestehende, internationale Standards vollständig akzeptiert werden oder alternativ besteht die Möglichkeit, dass das BFE eine Abwandlung eines bereits bestehenden, internationalen Standards oder gar einen komplett eigens entwickelten Standard für Cyber-Sicherheit und Resilienz im Stromsektor Schweiz definiert.
			L	▂▁▁	**S08.2** Die neue Regelung, welche eine (Teil-)Auslagerung der Prüftätigkeit an akkreditiere Drittstellen durch die Anerkennung von Zertifizierungen ermöglicht, ist gültig.
			L	▂▁▁	**S08.3** Akkreditierte Drittstellen prüfen Marktakteure und reichen die Prüfberichte – die Ausstellung eines Zertifikates – für den Überprüften im Rahmen der regelmässigen Überprüfung bei der Prüfbehörde ein. Die entsprechenden Prozesse und Fähigkeiten, um diese (Teil-)Auslagerung zu ermöglichen, sind bei der Prüfbehörde eingerichtet.
9	Das BFE und die Prüfbehörde setzen ‘**Incentives’ und/oder Sanktionierungen** ein, um Cyber-Anforderungen durchzusetzen.	M8	K	▂▄▁	**S09.1** Die nötigen Details und Konzepte sind erarbeitet. Es ist festgelegt, welche Formen der ‘Incentivierungen’ (z.B. Verrechenbarkeit der Kosten, Direktzahlungen, Unterstützung mit Know-How) / Sanktionierungen (z.B. Bussgelder) geeignet sind. Die rechtlichen Rahmenbedingungen zur Ermöglichung dieser Tätigkeit sind in der Gesetzgebung identifiziert.
			L	▂▁▁	**S09.2** Die neue gesetzliche Regelung tritt in Kraft.
			L	▂▄▁	**S09.3** Die Prüfbehörde und das BFE setzen in enger Zusammenarbeit basierend auf den Ergebnissen der regelmässigen Überprüfung bei den Betrieben kontinuierlich ‘Incentives’ und/oder Sanktionierungen ein.

Tabelle 17: Gantt-Diagramm - Überprüfung

#	Bis Ende 2022 (K)	Nach 2022 (L)
S04.1 Ausgestaltung & Verankerung des Registrierungsprozesses		
S04.2 Neue Regelung tritt in Kraft		
S04.3 Registrierung relevanter Marktteilnehmer		
S05.1 Prüfung rechtlicher Befugnisse & Ausgestaltung Überprüfungstätigkeit		
S05.2 Neue Regelung tritt in Kraft		
S05.3 Regelmässige Überprüfungen bei relevanten Unternehmen		
S06.1 Prüfung rechtlicher Befugnisse für Stichprobenkontrollen		
S06.2 Neue Regelung tritt in Kraft		
S06.3 Instandhaltung & Weiterentwicklung Stichprobenkontrollen		
S07.1 Ausarbeitung Selbstbeurteilungen		
S07.2 Klärung Informationsteilung von Selbstbeurteilungen		
S07.3 Neue Regelung tritt in Kraft		
S07.4 Aufrechterhaltung & Weiterentwicklung Selbstbeurteilungen		
S08.1 Prüfung Auslagerung der Überprüfungstätigkeit(en) an Dritte		
S08.2 Neue Regelung tritt in Kraft		
S08.3 Akkreditierte Drittstellen prüfen Marktakteure und Einreichen der Resultate		
S09.1 Grundlagenerarbeitung & rechtliche Abklärung betreffend 'Incentives' und/oder Sanktionierungen		
S09.2 Neue Regelung tritt in Kraft		
S09.3 'Incentives' und/oder Sanktionierungen kontinuierlich im Rahmen der Überprüfung eingesetzt		

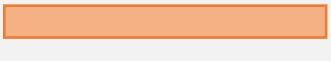
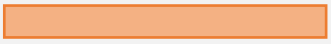
5.3 Meldewesen

Betreffend Meldewesen würden sich aus den vorgeschlagenen Optionen in Kapitel 4.3 die nachfolgenden Schritte ergeben.

Tabelle 18: Umsetzung der vorgeschlagenen Optionen - Meldewesen

#	Vorgeschlagene Option	NCS	Zeitspanne	Aufwand	Schritte zur Erreichung der Option
10	Es besteht eine unverzügliche **Meldepflicht** aller relevanten Marktteilnehmer an das NCSC **bei Cyber-Vorfällen**. Der Grundsatzentscheid des Bundesrats Ende 2020 und der kommende Entscheid spezifisch für den Stromsektor im April 2021 sind bei der Ausarbeitung dieses Vorschlags wegweisend.	M9	K	▂▄▆	**S10.1** Die Details zur Umsetzung der Meldepflicht im Stromsektor und die gesetzlichen Anforderungen der Meldepflicht sind identifiziert.
			L	▂▁▁	**S10.2** Die erarbeitete Meldepflicht ist verbindlich für die betroffenen Marktteilnehmer eingesetzt und die Unternehmen sind verpflichtet sich unverzüglich bei wesentlichen Cyber-Vorfällen bei dem NCSC zu melden.
			L	▂▄▁	**S10.3** Die neue Meldepflicht wird in der Praxis umgesetzt, wobei dem NCSC als Meldestelle eine wesentliche Rolle zukommt.
11	Das BFE und die Prüfbehörde setzen '**Incentives' und/oder Sanktionierungen** ein, um die Meldepflicht durchzusetzen.	M9	K	▂▄▁	**S11.1** Die spezifischen Massnahmen zur Sanktionierung und Incentivierung sind erarbeitet und die rechtlichen Rahmenbedingungen zur Ermöglichung dieser Tätigkeit sind in der Gesetzgebung identifiziert. Es ist festgelegt, welche Formen der 'Incentivierungen' (z.B. Verrechenbarkeit der Kosten, Direktzahlungen, Unterstützung mit Know-How) / Sanktionierungen (z.B. Bussgelder) geeignet sind.
			L	▂▁▁	**S11.2** Die gesetzliche Regelung tritt in Kraft.
			L	▂▄▁	**S11.3** Das BFE und die Prüfbehörde arbeiten eng zusammen, um entweder den Unternehmen Anreize für allfällige Meldungen zu ermöglichen und/oder bei einer Nicht-Einhaltung der Meldepflicht zu strafen.

Tabelle 19: Gantt-Diagramm - Meldewesen

#	**Bis Ende 2022** (K)	**Nach 2022** (L)
S10.1 Grundlagenerarbeitung & rechtliche Abklärung betreffend Meldepflicht		
S10.2 Neue Regelung tritt in Kraft		
S10.3 Relevante Marktakteure melden Cyber-Vorfälle unverzüglich bei NCSC		
S11.1 Grundlagenerarbeitung & rechtliche Abklärung betreffend 'Incentives' und/oder Sanktionierungen		
S11.2 Neue Regelung tritt in Kraft		
S11.3 'Incentives' und/oder Sanktionierungen kontinuierlich im Rahmen der Meldepflicht eingesetzt		

5.4 Wissensaustausch

Zur Umsetzung des Wissensaustausches gemäss Kapitel 4.4 wären die untenstehenden Schritte zu berücksichtigen.

Tabelle 20: Umsetzung der vorgeschlagenen Optionen - Wissensaustausch

#	Vorgeschlagene Option	NCS	Zeit-spanne	Auf-wand	Schritte zur Erreichung der Option
12	Das BFE verarbeitet die erhaltene Threat Intelligence vom NCSC für die **(Weiter-)Entwicklung von Cyber-Anforderungen**.	M4	L	▂□□	**S12.1** Die Methodik und der Mechanismus zur situativen Anpassung der Regulierung basierend auf der erhaltenen Threat Intelligence ist ausgearbeitet.
			L	▂□□	**S12.2** Die Fähigkeiten innerhalb des BFE für eine solche Tätigkeit sind umgesetzt und wird fortwährend gefördert.
13	Das **BFE erstellt Handlungsempfehlungen und Hilfestellungen für Marktteilnehmer** im Sinne einer Interpretation des Gesetzgebers betreffend die aktuelle Gefahrenlandschaft und adäquate Reaktion durch Marktteilnehmer.	M4	L	▂□□	**S13.1** Die fachlichen Kompetenzen beim BFE bestehen, damit die relevanten Entwicklungen identifiziert, mögliche Massnahmen beurteilt, und entsprechend veranlasst werden.

Tabelle 21: Gantt-Diagramm - Wissensaustausch

#	K	L
S12.1 Ausarbeitung Methodik & Mechanismus für Weiterverarbeitung Threat Intelligence		
S12.2 Aufbau Threat Intelligence Fähigkeiten für (Weiter-)Entwicklung von Cyber-Anforderungen bei BFE		
S13.1 Aufbau Threat Intelligence Fähigkeiten für Handlungsempfehlungen und Hilfestellungen für Marktteilnehmer		

5.5 Zusammenfassung

Abschliessend wären kurzfristig zwingend die Rollen und Kompetenzen der zuständigen Behörden zu klären und schliesslich auch rechtlich zu verankern. Die Mandate sollten abschliessend gesichert sein, um das weitere Vorgehen zu ermöglichen. Weiter sollten in absehbarer Zeit die verpflichtenden Cyber-Anforderungen vom BFE für die relevanten Marktteilnehmer definiert und rechtlich begründet werden.

Betreffend Meldewesen, wird für den Stromsektor derzeit bereits an einer sektorspezifischen Meldepflicht gearbeitet und voraussichtlich im April 2021 definitiv verabschiedet. Dieser Entscheid und die Beauftragung des Bundesrats an das EFD, bis Ende 2021 eine Vernehmslassungsvorlage auszuarbeiten, bilden die rechtlichen Grundlagen für die vorgeschlagene Meldepflicht. Letztlich wäre kurzfristig auch die Zusammenarbeit mit dem NCSC zu institutionalisieren, damit eine nachhaltige, fachbezogene Kooperation zwischen den staatlichen Akteuren eingesetzt werden könnte. Diese initialen Schritte würden die Grundlage für alle nachfolgenden Handlungsfelder bilden.

Mittelfristig müssten alle neuen, gesetzlichen Regelungen entsprechend in Kraft treten. Die neu definierten Anforderungen würden dadurch für die relevanten Marktteilnehmer verbindlich und müssen implementiert werden. Auch müssten parallel die jeweiligen internen Prozesse, Systeme und Tätigkeiten auf Seiten des BFE und der künftigen Prüfbehörde festgelegt und implementiert werden.

Das untenstehende Gantt-Diagramm verdeutlicht alle zwingenden, kurzfristigen Schritte, welche vor Ende 2022 angegangen werden sollten, damit die NCS 2018-2022 erfolgreich abgeschlossen werden kann.

Tabelle 22: Zusammenfassung - Gantt-Diagramm für alle zwingenden, kurzfristigen Schritte

	#	**Bis Ende 2022** (K)
Grundlagen	**S01.1** Abgrenzung von Rollen & Verantwortlichkeiten im Bereich Cyber	
Rahmenbedingungen	**S03.1** Identifikation von Cyber-Anforderungen	
Überprüfung	**S04.1** Ausgestaltung & Verankerung des Registrierungsprozesses	
	S05.1 Prüfung rechtlicher Befugnisse & Ausgestaltung Überprüfungstätigkeit	
	S09.1 Grundlagenerarbeitung & rechtliche Abklärung betreffend 'Incentives' und/oder Sanktionierungen	
Meldewesen	**S10.1** Grundlagenerarbeitung & rechtliche Abklärung betreffend Meldepflicht	
	S11.1 Grundlagenerarbeitung & rechtliche Abklärung betreffend 'Incentives' und/oder Sanktionierungen	

Zusammenfassend stellt Tabelle 23 den mit den vorgeschlagenen Optionen angezielten Umsetzungsstand (= U. in Tabelle) dar. Es ist deutlich, dass die Optionen erheblich zu der Erreichung der NCS 2018-2022 beitragen.

Tabelle 23: Übereinstimmung der NIS-Richtlinie, der NCS 2018-2022 und den vorgeschlagenen Optionen

EU NIS Verpflichtung			Mapping NCS 2018-2022	Aktuell U.	Ziel U.	Identifizierter Handlungsbedarf für den Schweizer Stromsektor gemäss vorgeschlagener Zielzustand
# 1	Nationale Strategie		**Verabschiedung der NCS 2018-2022**	✓	✓	(Keiner)
# 2	EU-Kooperationsgruppe		Nicht direkt anwendbar, da kein EU-MS und daher nicht Mitglied der Gruppe.			
# 3	Netzwerk von Computer-Notfallteams		Nicht direkt anwendbar, da kein EU-MS, aber gewisse Relevanz für GovCERT.ch			
# 4	Sicherheitsanforderungen und Meldepflichten	Sicherheitsanforderungen	**NCS Massnahme 8**	✗	✓	Kapitel 4.1 «Rahmenbedingungen» *Zwingend*: #3 Schaffung Cyber-Anforderungen *Optional*: -
		Meldepflicht	**NCS Massnahme 9**	✗	✓	Kapitel 4.3 «Meldewesen» *Zwingend*: #10 Meldepflicht, #11 'Incentives' und/oder Sanktionierungen *Optional*: -
		Überprüfung	**Impliziert duch NCS Massnahmen 8**	✗	✓	Kapitel 4.2 «Überprüfung» *Zwingend*: #4 umfassende Überprüfung, #5 Registrierung, #9 'Incentives' und/oder Sanktionierungen *Optional*: #6 Stichprobenkontrollen, #7 Externe Prüfstellen, #8 Selbstbeurteilungen
# 5	Ernennung von:	Nationale zuständige Behörden	**Allgemeine Bestimmungen der NCS und NCS Umsetzungsplan**	↔	✓	Grundlegend für alle Bereiche *Zwingend*: #1 Zuständigkeiten BFE & Prüfbehörde *Optional*: #2 Zusammenarbeit NCSC
		Zentrale Anlaufstelle	**Schaffung NCSC im Rahmen der NCS**	✓	✓	(Keiner)
		Nationales CERT	**NCS Massnahme 4**	↔	✓	Kapitel 4.4 «Wissensaustausch» *Zwingend*: - *Optional*: #12 (Weiter-)Entwicklung Regulierung, #13 Sektor-spezifische Hilfestellungen

Fazit Kapitel 5 - Umsetzung der vorgeschlagenen Optionen zur Adressierung des Handlungsbedarfs

Der grobe Umsetzungsplan zeigt die verschiedenen kurz- und langfristigen Schritte auf, welche bei der Implementierung des gesamtheitlichen Cyber-Sicherheit und Resilienz Konzepts für den Schweizer Strommarkt zwingend und/oder optional anzuwenden sind.

Zunächst und grundlegend müssen die ersten kurzfristigen Schritte auf die Klärung der rechtlichen Mandate/Aufgaben und Kompetenzen der zuständigen Behörden abzielen. Sodann kann grob folgendes Vorgehen gewählt werden. Die relevanten Markteilnehmer sollten identifiziert werden und in einem ein Register aufgenommen werden. Zur Erhöhung der «Awareness» sollten regelmässige, verpflichtende Selbstbeurteilungen erfolgen. Parallel dazu wäre die Identifikation der Cyber-Anforderungen und die Ausgestaltung der Überprüfung anzugehen. Hierbei empfiehlt es sich schrittweise vorzugehen, um die Akzeptanz hoch zu erhalten und die Erkenntnisse der Selbstbeurteilungen laufend in die Arbeiten einfliessen zu lassen.

Langfristig treten anfangs diese neuen gesetzlichen Regelungen in Kraft. Die entsprechenden Prozesse, Systeme und Tätigkeiten werden fortan stets weiterentwickelt, um zukünftige technologische Entwicklungen und digitale Innovationen laufend zu berücksichtigen.

Die Schritte sind durchaus ambitiös ausgelegt und müssen weiter in Zusammenarbeit mit den betroffenen Akteuren verfeinert werden. Es ist aber eindeutig, dass die vorgeschlagenen Elemente erheblich zu der Erreichung der NCS 2018-2022 beitragen, dadurch den Schweizer Stromsektor effektiv vor den steigenden Cyber-Risiken schützen können und die Versorgungssicherheit auch im Zuge der fortschreitenden Digitalisierung nachhaltig schützen können.

Ausblick und Fazit des Berichts

«Die digitale Transformation wird den Energiesektor grundlegend, langfristig und nachhaltig verändern. Sie verändert spezifische Bereiche, wirkt aber oft besonders im Querschnitt.»[87]

Wie bereits in der Einleitung aufgeführt, ermöglicht die Digitalisierung dem Stromsektor immense Opportunitäten. Beispielsweise können neue Dienstleistungen angeboten werden, die Einführung erneuerbarer Energien unterstützt, sowie der derzeitige Ressourceneinsatz optimiert werden. Diese Entwicklungen machen den Energiesektor jedoch auf unterschiedliche Art und Weise zunehmend verletzbarer und angreifbarer für Cyber-Attacken.

Neuere Entwicklungen der Digitalisierung im Stromversorgungsbereich müssen künftig laufend betreffend ihren Einfluss auf die Cyber-Sicherheit und Resilienz des Schweizer Stromsektors im Auge behalten werden. Nur so können rechtzeitig entsprechende Massnahmen und Anpassungen forciert werden, um ein adäquates Schutzniveau des Sektors weiterhin zu gewährleisten. Insbesondere die folgenden, neueren technologischen Entwicklungen sollten nicht ausser Acht gelassen werden und dürften eine gewisse Reaktion künftig erfordern.

«Internet of Things» (IoT) und «5G» Funktechnologie

Die maschinelle und auf Automatisierung basierte Vernetzung von Geräten, ist ein wesentlicher Treiber der digitalen Transformation. Die meisten Komponenten des Energiesektors – Smart Meter, dezentrale Stromerzeugungs- und Speichergeräte, Haushaltsgeräte, Elektroautos, aber auch aktive Netzkomponenten wie spannungsgeregelte Transformatoren – werden so zunehmend digital vernetzt und voneinander abhängig. Die Angriffsfläche für Cyber-Attacken steigt daher rasant an. Das so genannte «Weakest Link Problem» – ein zentrales Konzept der Informationssicherheit – zeigt auf, dass ein Netz meist nur so sicher ist, wie der schwächste Teil des gesamten Systems. Das Zusammenwachsen aller Komponenten in ein grosses Netzwerk führt dazu, dass die Verbreitung künftiger Cyber-Vorfälle immer einfacher schneller von statten gehen wird und eine grössere Reichweite hat.

5G-Funkverbindungen wird die Digitalisierung im Energiesektor zusätzlich vorantreiben und die bereits oben genannten Herausforderungen nochmals zusätzlich verstärken.

«Artificial Intelligence» (AI)

Der Einsatz künstlicher Intelligenz hat in Bezug auf die Cyber-Sicherheit sowohl positive, als auch negative Aspekte. So ermöglicht die Nutzung von künstlicher Intelligenz beispielsweise eine Erweiterung der automatisierten Reaktionshandlungen von Maschinen auf Vorfälle[88], kann aber auch im negativen Sinne genutzt und missbraucht werden – beispielsweise eine automatisierte Durchsuchung von Netzwerkstrukturen und -aktivitäten für Spionagezwecke oder für eine effizientere und präzisere Durchführung von Cyber-Attacken.

---

87 Bundesamt für Energie (2018, S. 8), Digitalisierung im Energiesektor: Dialogpapier zum Transformationsprozess.

88 Vgl. EU ‘cybersecurity shield' («Cyber-Sicherheitsschutzschild»), welches frühzeitige Signale für drohende Cyber-Angriffe erkennen und die entsprechenden Massnahmen ermöglichen soll, bevor Schäden verursacht werden (Kapitel 2.2.1 Einführung zur NIS-Richtlinie).

Im Energiesektor kann künstliche Intelligenz beispielsweise angewendet werden, um die Prognosen betreffend Energieerzeugung und -verbrauch zu verbessern und die jeweilige Netzlast besser zu steuern. Die Technologie kann so unter anderem dazu beitragen, erneuerbare Energien zu integrieren und die Stabilität des Energiesystems zu erhöhen. Zusätzlich fördert künstliche Intelligenz die Identifikation von Cyber-Attacken, deren Anwendung es ermöglicht auffällige Muster bei digitalen Prozessen aus Energieerzeugung, -transport, -handel oder -verbrauch zu erkennen. Die erwartungsgemäss grösste negative Auswirkung der künstlichen Intelligenz im Energiesektor ist die Steigerung der Fähigkeiten krimineller Akteure. Beispielsweise könnten durch die Verwendung von künstlicher Intelligenz vorhandene Sicherheitslücken um einiges schneller als bisher identifiziert werden, indem Benutzerverhalten analysiert, Muster erkannt und Unregelmässigkeiten im Netzwerk identifiziert und entsprechend ausgenützt werden.

«Big Data» und «Cloud»

«Big Data», respektive die Sammlung und Auswertung von grossen Mengen an Daten und Informationen betrifft den Stromsektor insbesondere bei der Integration von Smart Metern und anderen intelligenten Produkten (vgl. IoT), da anhand der gesammelten Daten die Bedürfnisse der Verbraucher gezielt optimiert werden können. Dies bedeutet jedoch, dass der entsprechende Datenschutz aus einer Cyber-Sicherheitsperspektive immer wichtiger wird, damit die Privatsphäre der Nutzer entsprechend geschützt werden kann. Nicht zuletzt dienen Massnahmen der Informationssicherheit auch einem guten Datenschutz und sind dahingehend ein integraler Teil des kürzlich revidierten Datenschutzgesetzes (DSG). Auch vor diesem Hintergrund sind zusätzliche Massnahmen im Bereich der Cyber-Sicherheit keine Frage des «kann», sondern des «muss».

Cloud Technologie**,** und insbesondere die Nutzung von virtuellem Speicher (Cloud Storage), ermöglicht es, grosse Datenmengen anzusammeln und gleichzeitig für eine Vielzahl von Benutzer verfügbar zu machen. Dies begünstigt unter anderem neue Steuerungsmöglichkeiten der multidirektionalen Elektrizitätsflüsse dank Echtzeitübermittlungen, sowie die vereinfachte, direkte Integration von neuen stromproduzierenden Konsumenten.

Für die Cyber-Sicherheit im Energiesektor bedeutet dies, dass Marktteilnehmer wahrscheinlich zunehmend Dienstleistungen von externen Cloud-Anbietern in Anspruch nehmen werden. Dies bedeutet aber nicht, dass die Verantwortung für Cyber-Sicherheit mit dieser Auslagerung abgegeben wird. Zukünftige Anforderungen sollten daher zwingend auch Massnahmen betreffend Lieferketten-Risikomanagement beinhalten («Third Party Risk Management»).

Dieser Ausblick auf zukünftige Herausforderungen der Cyber-Sicherheit durch die fortschreitende Digitalisierung ist nicht abschliessend. Technologische Entwicklungen und digitale Innovationen sind laufend zu berücksichtigen und in das angestrebte Cyber-Sicherheits- und Resilienz-Regelwerk einzuarbeiten.

Gesamtfazit des Berichts

Die Thematik rund um die Bereiche Cyber-Sicherheit und Resilienz wird zu einem immer zentraleren Bestandteil der Schweizer Elektrizitäts-Versorgungssicherheit. Durch die zunehmende Anwendung digitaler Technologien, wie beispielsweise der Einsatz intelligenter Messsysteme (Smart Meter), findet eine immer stärker werdende Vernetzung der Stromnetze statt. Gleichzeitig fördert dies eine zunehmende Verschmelzung der Informationstechnologie- (IT) und der operationellen Technologie-Landschaft (OT) zum Betreiben der Netze und Werke.

Eine klassische, physische Trennung der beiden Welten ist daher nicht mehr gegeben und es entstehen neue, bisher nicht da gewesene Angriffsvektoren. Cyber-Angriffe werden immer wahrscheinlicher und die Auswirkungen können unter anderem aufgrund von Kaskadeneffekten und der «Weakest Link»-Problematik vermehrt systemrelevante Folgen haben. Die Cyber-Bedrohungslage steigt also rasant an und hat sich während der Corona-Pandemie nochmals zusätzlich verschärft.

Historisch gesehen wurde das Schweizerische Stromversorgungssystem auf eine Art und Weise erschaffen und reguliert, um primär auf Bedrohungsszenarien der physischen Sicherheit einzugehen. Existierende Schutzkonzepte müssen entsprechend der neuen Ausgangslage überarbeitet werden, damit künftige Krisensituationen wie beispielsweise dem Auftreten grossflächiger «Blackouts» auch weiterhin möglichst erfolgreich vermieden werden können und die sichere Landesversorgung mit Elektrizität entsprechend garantiert ist.

Zweck dieses vorliegenden Berichts war deshalb die Erarbeitung eines gesamtheitlichen Konzepts für Cyber-Sicherheit und Resilienz im Schweizer Stromsektor. Mit dem Bericht wurden erste Grundlagen geschaffen, um generell die Maturität aller Akteure innerhalb der Schweizer Stromversorgung bezüglich Cyber-Sicherheit über die Zeit zu erhöhen und dadurch den Sektor künftig besser auf neue Cyber-Gefahren vorzubereiten.

Bei der Erarbeitung des Berichts wurde zunächst festgestellt, dass die Schweiz aktuell bereits über mehrere Ansätze und regulatorische Grundlagen für Cyber-Sicherheit und Resilienz im Schweizer Stromsektor verfügt. Es besteht jedoch eine starke Fragmentierung, da diese Thematik aktuell noch nicht einheitlich, flächendeckend und umfassend für alle Akteure geregelt ist. Bereits bestehende, Cyber-bezogene Auflagen und Pflichten für einzelne Akteure sind weit verstreut innerhalb verschiedener Gesetzestexte festgehalten und eine transparente Gesamtübersicht fehlt. Der IKT Minimalstandard des BWL und das OT-Handbuch des VSE fördern ein erstes Grundverständnis für den Themenbereich, geben jedoch nur freiwillige Richtlinien vor. Der Bund hat diesen Missstand erkannt und gibt entsprechend mittels der Nationalen Strategie zum Schutz vor Cyber-Risiken 2018-2022 (NCS) eine strategische Richtung vor.

Zwei Entwicklungen seit der Verabschiedung der NCS 2018-2022 waren für die Ausarbeitung des Konzepts wesentlich. Erstens ist der Beschluss des Bundesrats, dass, basierend auf einem Bericht der der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit, verpflichtende Sicherheitsstandards zu prüfen und bis Ende 2022 Lösungsoptionen aufzuzeigen sind, hervorzuheben. Es wird dabei gefordert, dass Bund und Kantone in enger Zusammenarbeit mit den Fachverbänden auditierbare IKT-Sicherheitsstandards erarbeiten und die Betreiber von KI verpflichten, diese Sicherheitsstandards einzuhalten. Zweitens, hat sich der Bundesrat im Dezember 2020 für die Einführung einer Meldepflicht für KI bei Cyber-Angriffen ausgesprochen. Der Bundesrat hat das EFD beauftragt, bis Ende 2021 eine Vernehmlassungsvorlage auszuarbeiten, welche die rechtlichen Grundlagen für diese Meldepflicht schafft. Eine Stromsektor-spezifische Vorgabe bezüglich Meldepflicht wird im April 2021 erwartet.

Im Quervergleich mit anderen Ländern betreffend regulatorische Situation für Cyber-Sicherheit und Resilienz im jeweiligen Stromsektor wurde erkannt, dass viele Länder aktuell eine ähnliche Stossrichtung verfolgen, jedoch gegenüber der Schweiz einen gewissen Vorsprung vorweisen und häufig

bereits entsprechende Massnahmen in die Praxis umgesetzt haben. In den Vereinigten Staaten sind die Anforderungen beispielsweise besonders detailliert und weitreichend. In der Europäischen Union wird die NIS-Richtlinie aktuell bereits zum ersten Mal mit Hochdruck überarbeitet und weiterentwickelt. Die in näherer Zukunft vorgesehene Implementierung des «Cybersecurity Network Code» angestrebt durch ENTSO-E und EUDE, mit einer vorgeschlagenen Zertifizierung mindestens nach ISO27001 für alle Betreibe und zusätzlichen Anforderungen speziell für KI, beschleunigt diese Tendenz zusätzlich.

Die Entwicklungen der EU sind insbesondere daher spannend, da eine sehr starke technische und organisatorische Vernetzung der verschiedenen Stromsysteme der Schweiz und der EU-Mitgliedstaaten besteht, vor allem mit den unmittelbaren Nachbarländern der Schweiz. Entsprechend gross sind die wechselseitigen Abhängigkeiten voneinander und der Bedarf einer Angleichung bestehender regulatorischer Anforderungen. So ist es auch nicht weiter verwunderlich, dass die in der NCS 2018-2022 festgehaltenen Stossrichtungen des Bundes grösstenteils mit den beschriebenen Massnahmen der NIS-Richtlinie der EU kompatibel sind. Die Massnahmen sind weitgehend deckungsgleich, wenn auch die Vorgaben der NIS1-Richtlinie bereits um einiges konkreter ausgearbeitet sind. Es wurden schliesslich vier Handlungsfelder identifiziert, in welchen der Schweizer Stromsektor gemäss der NCS 2018-2022 momentan gewisse Lücken aufweist.

Als Teil dieses Berichts wurde komplementär ebenfalls eine elektronische Umfrage (E-Survey) durchgeführt, um unter anderem den aktuellen Cyber-Maturitätsstand der verschiedenen Akteure des Schweizer Stromsektors zu verstehen und zu sehen, ob der im Vergleich mit dem Ausland identifizierte Rückstand der Schweiz sich auch in der Praxis derzeit negativ auswirkt. Die Auswertungsresultate der Umfrage zeigen ein Bild, welches diese Annahme bestätigt. Im Schnitt war das allgemeine Maturitätsniveau der Schweizer Stromversorger tief. Cyber-Risiken werden offenbar meist ad-hoc und entsprechend reaktiv verwaltet. Risikomanagementprozesse und organisatorische Vorgaben zur IKT-Sicherheit scheinen daher meist nicht formalisiert.

Infolgedessen hat dieser Bericht als Resultat dieser Analysen und Umfrage primär vier Handlungsfelder gemäss NCS 2018-2022 identifiziert, bei welchen der Schweizer Stromsektor aktuell grossen Weiterentwicklungsbedarf hat. Diese sind:

1) *das Schaffen einheitlicher, gesetzlicher Rahmenbedingungen*: risikobasierte und verbindliche Anforderungen sollten für alle relevanten Unternehmen der Elektrizitätswirtschaft vom BFE eingesetzt werden. Die Anforderungen wären selektiv auf Basis von bestehenden nationalen Grundlagen und internationalen Frameworks und Standards zu erarbeiten.

2) *die regelmässige Überprüfung der Einhaltung regulatorischer Anforderungen*: betroffene Marktteilnehmer des Stromsektors Schweiz sollten in regelmässigen Abständen auf ihre Gesetzeskonformität von einer Prüfbehörde mithilfe unterschiedlicher Mechanismen geprüft werden.

3) *der institutionalisierte, regelmässige Wissensaustausch betreffend aktuelle Cyber-Gefahren* (Threat Intelligence): dies würde die Bereitstellung von konkreten Hilfsstellungen an die Marktteilnehmer ermöglichen, sowie könnte dabei helfen die Cyber-Anforderungen langfristig an die Cyber-Bedrohungslage anzupassen; und

4) *das institutionalisierte Meldewesen betreffend laufender Cyber-Attacken innerhalb des Stromsektors Schweiz*: eine Meldepflicht für wesentliche Cyber-Vorfälle ist gemäss dem Bundesratsentscheid Ende 2020 und der kommenden sektorspezifischen Regelung einzuführen, um die Risikolage genauer einschätzen und Gefahren besser bekämpfen zu können.

Entlang dieser vier Handlungsfelder wurde mittels dieser Arbeit ein initiales, ganzheitliches Konzept zur künftigen Umsetzung von Cyber-Sicherheit und Resilienz im Schweizer Stromsektor erarbeitet,

welches mögliche Handlungsoptionen und Massnahmen zur künftigen Stärkung des Sektors im Cyber-Bereich transparent aufzeigt, sowie konkrete Handlungsempfehlungen abgibt.

Im Anschluss wurde ein grober Umsetzungsplan skizziert, wie die empfohlenen Massnahmen künftig umgesetzt werden könnten. Zunächst und grundlegend sollten die ersten kurzfristigen Schritte auf die Klärung der rechtlichen Mandate/Aufgaben und Kompetenzen der zuständigen Behörden abzielen. Grundlagenerarbeitungen und rechtliche Abklärungen sollten somit die ersten Aktivitäten nach der Veröffentlichung dieses Berichts prägen. Es ist hierbei ebenfalls anzumerken, dass die Mehrheit der Massnahmen gleichzeitig von zentraler Bedeutung ist, um die vorgegebene NCS 2018-2022 des Bundes innerhalb des Schweizer Stromsektors erfolgreich umzusetzen. Des Weiteren sind technologische Entwicklungen und digitale Innovationen auch künftig weiterhin stets für eine erfolgreiche Umsetzung zu berücksichtigen und in das angestrebte Cyber-Sicherheits- und Resilienz-Konzept des Stromsektors Schweiz laufend miteinzuarbeiten.

Glossar

Begriff	Bedeutung
Computer Emergency Response Team (CERT)	Die Kernaufgabe eines CERT ist die Prävention, Detektion und Bewältigung von IT- und Netzwerk-Vorfällen, welche seine Kunden betreffen. Das CERT-Team besteht aus IT-Sicherheitsspezialisten und arbeitet eng und auf hohem Vertrauensniveau mit seinen Kunden zusammen. Aufgrund der internationalen Dimension benötigt ein CERT-Team neben einem sehr guten nationalen auch ein weltweites Netzwerk von Vertrauensbeziehungen auf operativer IT-Security-Ebene. Im Gegensatz zu SOCs, sind CERTs eher eine Notfallorganisation, welche sich um detaillierte Analysen und sich mit der Behebung von Sicherheitsvorfällen beschäftigt. SOC und CERT ergänzen sich und bilden somit eine leistungsfähige Einheit für die Cyber-Sicherheit. CERT und CSIRT wurden in dem Bericht synonym verwendet.
Cyber-Sicherheit	Cyber-Sicherheit, engl. cyber security, befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Die Bereiche der IT- und OT-Sicherheit werden als zwei zentrale Unterkategorien der gesamtheitlichen Cyber-Sicherheit (wie auch Cyber-Resilienz) anerkannt. Die Informationssicherheit und Datensicherheit sind als Teilbereiche der Cyber-Sicherheit zu verstehen.
Cyber-Resilienz	Cyber-Resilienz impliziert die Annahme, dass kein vollständiger Schutz vor Cyber-Risiken möglich ist, die Risiken aber soweit behandelt werden können, dass das verbleibende Risiko tragbar ist. Deshalb wird die Cyber-Resilienz als weiterführendes, zentrales Element für ein gesamtheitliches Konzept Cyber-Sicherheit und Cyber-Resilienz für den Schweizer Strommarkt eingesetzt.
Defense-in-Depth Strategie	Darunter versteht man einen koordinierten Einsatz mehrerer Sicherheitsmassnahmen, um die IKT-Betriebsmittel in einem Unternehmen zu schützen. Die Strategie basiert auf dem militärischen Prinzip, dass es für einen Feind schwieriger ist, ein komplexes und mehrschichtiges Abwehrsystem zu überwinden als eine einzige Barriere.
Information Technology (IT)	Technologien zur Datenverarbeitung, welche nicht direkt mit der Bereitstellung von Elektrizität zu tun haben.

	z.B. Kundendatenmanagement, Personaldatenmanagement, Büroanwendungen
Informationssicherheits-Managementsystem (ISMS)	Unternehmensweit wirkendes Managementsystem, das die Einhaltung des Sicherheits- und Kontinuitätsniveaus von Informationen nachhaltig und effektiv sicherstellt.
Internet of Things (IoT)	Bei IoT geht es um die Vernetzung von Objekten übers Internet, wie z.B. Industriemaschinen, Autos, TV's und Waschmaschinen. Durch diese Vernetzung und die immer grössere Verbreitung von Sensoren in den (Alltags-) Objekten entstehen Milliarden "intelligenter Gegenstände". Eine einheitliche Definition von IoT hat sich unter den unterschiedlichen Akteuren jedoch noch nicht durchgesetzt.
Korrelation	Korrelationen beschreiben eine Beziehung zwischen zwei oder mehreren Merkmalen, Zuständen oder Funktionen. Die Beziehung muss keine kausale Beziehung sein, d.h. manche Elemente eines Systems beeinflussen oder begründen sich gegenseitig nicht.
Malware	Malware ist ein Sammelbegriff für Programme, welche dazu entwickelt wurden, Benutzern Schaden zuzufügen. Es gibt zahlreiche Unterarten von Malware, z.B., Viren, Trojaner oder Spyware. Alle verlaufen anders und haben verschiedene Aufgaben, aber das gemeinsame Ziel den Benutzern zu schaden.
Operational Technology (OT)	Technologien, welche direkt für die Bereitstellung oder Lieferung von Elektrizität notwendig sind. z.B. Supervisory Control and Data Acquisition (SCADA), Fernzugriff auf Installationen in Unterwerken, Rundsteuerung, Energiedatenmanagement, Smart Meter
Security Information and Event Management (SIEM)	Das SIEM ermöglicht einen ganzheitlichen Blick auf die IT-Sicherheit, indem Meldungen und Logfiles verschiedener Systeme gesammelt und ausgewertet werden. Verdächtige Ereignisse oder gefährliche Trends lassen sich in Echtzeit erkennen.
Security Operations Center (SOC)	Ein SOC ist eine Zentrale für alle sicherheitsrelevanten Services im IT-Umfeld von Unternehmen. Das SOC integriert, überwacht und analysiert alles sicherheitsrelevanten Systeme wie Unternehmensnetzwerke, Server oder Internetservices. Unter anderem werden die Log-Dateien der einzelnen Systeme gesammelt, analysiert und nach Auffälligkeiten unter-sucht.
Single Point of Contact (SPoC)	Dezidierter Ansprechpartner / Kontaktperson für Cyber-Sicherheit bei einem Unternehmen.
Supervisory Control and Data Acquisition (SCADA)	SCADA sind industrielle Kontrollsysteme und ein Überbegriff für all diejenigen Elemente, die zur Steuerung und Überwachung von Anlagen oder Industrieprozessen eingesetzt werden. Ein industrielles Kontrollsystem

	umfasst typischerweise Sensoren, Rechenzentren, Leitstellen, Leitungen und Anlagen.
Smart Grid	Ein Smart Grid ist ein System, das den Austausch elektrischer Energie aus verschiedenartigen Quellen mit Konsumenten verschiedener Verbrauchsprofilen intelligent sicherstellt, d.h. unter Einbezug von Messtechnologien sowie IKT.
Smart Meter	«Smart Meter» sind intelligente Messsysteme, die über eine bidirektionale Kommunikation ihre Messdaten übertragen und Steueraufgaben übernehmen können. Diese Systeme bieten dem Netzbetreiber mehr Steuerungsmöglichkeiten und ermöglichen einen effizienteren Systembetrieb sowie die Möglichkeit neue Dienstleistungen anzubieten. Sie tragen zu einem einfachen Endverbraucher- und Mieterwechsel sowie einer stark vereinfachten Stromablesung bei. Die Visualisierung des Verbrauchs fördert Energieeffizienz (Stromeinsparungen) beim Endverbraucher und unterstützt die Verwaltung der dezentralen Produktion, z.B. innerhalb des Eigenverbrauchs.
Social Engineering	Social Engineering Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Aktionen zu bewegen. Ein Angreifer kann mittels Social Engineering beispielsweise versuchen, an Benutzernamen und Passwörter von Mitarbeitern eines Unternehmens zu gelangen, indem er sich am Telefon als Systemadministrator oder Sicherheitsverantwortlicher ausgibt. Durch Vorgeben akuter Computerprobleme und Vortäuschen von Betriebskenntnissen (z. B. Namen von Vorgesetzten, Arbeitsabläufe, usw.) wird das Opfer so lange verunsichert, bis es die gewünschten Informationen preis gibt.
Threat Intelligence	Threat Intelligence ist eine relativ junge Disziplin und ein solcher Service liefert aktuelle Informationen zur Cyber-Bedrohungslage damit Unternehmen einen Wissensvorsprung bezüglich wie und was für ein Angriff erfolgen könnte und sich entsprechend dagegen wappnen kann. Daraus ergeben sich unter Anderem konkrete Handlungsempfehlungen und Hilfestellungen für Marktteilnehmer.
Three-Lines-of-Defense-Modell	Das «Three-Lines-of-Defense»-Modell zeigt eine systematische Herangehensweise an Risiken für Unternehmen auf. Mit der zunehmenden Komplexität von Unternehmensstrukturen und der Gliederung in unterschiedliche Abteilungen, erlaubt das Modell eine Struktur aufzubauen, mit welcher ein gemeinsames und einheitliches Management von Risiken gefördert wird. Das Risikomanagement wird so effektiver, da die Kommunikation, sowie eine genaue Aufgabenidentifikation ver-

	bessert wird. «First-Line of Defense» betrifft das operative Management; «Second-Line-of-Defense» ist die Überwachung und Unterstützung der Ersten; «Third-Line-of-Defense» dient zur Revision all dieser Tätigkeiten.

Literaturverzeichnis

Agence nationale de la sécurité des systèmes d'information (2020), The French CIIP Framework. Abgerufen am 19.11.2020 von https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

Astley, Peter / Pundmann, Sandy / Regelbrugge, Adam (2020), Modernizing the three lines of defense model.

Barichella, Arnault (2018), Cybersecurity in the energy sector: a comparative analysis between Europe and the United States.

Bird & Bird (2020), Developments on NIS Directive in EU Member States.

Blueprint Energy Solutions GmbH (2019), Final Report - Study on cyber security in the energy sector of the Energy Community.

Bundesamt für Energie (2016a), Risiko- und Schutzbedarfsanalyse für Smart Grids.

Bundesamt für Energie (2016b), Risiko- und Schutzbedarfsanalyse für Smart Meter.

Bundesamt für Energie (2018), Digitalisierung im Energiesektor: Dialogpapier zum Transformationsprozess.

Bundesamt für Energie (2020), Digitalisierung im Energiesektor.

Bundesamt für wirtschaftliche Landesversorgung (2017), Risiko- und Verwundbarkeitsanalyse des Teilsektors Stromversorgung.

Bundesamt für wirtschaftliche Landesversorgung (2018), IKT Minimalstandard.

Bundesgesetz über die Stromversorgung (Stromversorgungsgesetz, StromVG) vom 23. März 2007 (Stand am 1. Juni 2019).

Bundesgesetz über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz, LVG) vom 17. Juni 2016 (Stand am 1. Januar 2020).

Bundesrat (2017), Nationale Strategie zum Schutz Kritischer Infrastrukturen 2018–2022.

Bundesrat (2018a), Medienmitteilung: Bundesrat nimmt Schlussbericht der Expertengruppe „Zukunft der Datenbearbeitung und Datensicherheit" zur Kenntnis.

Bundesrat (2018b), Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-2022.

Bundesrat (2019), Bericht: Varianten für Meldepflichten von Kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen.

Bundesrat (2020), Medienmitteilung: Bundesrat spricht sich für eine Meldepflicht für kritische Infrastrukturen bei Cyberangriffen aus.

Deutsche Akkreditierungsstelle (2020), Akkreditierung für IT-Sicherheitskatalog nach EnWG. Abgerufen am 19.11.2020 von https://www.dakks.de/content/weitere-akkreditierung-f%C3%BCr-it-sicherheitskatalog-nach-enwg-ab-sofort-m%C3%B6glich

Deutsche Bundesnetzagentur (2020), IT-Sicherheit im Energiesektor. Abgerufen am 15.10.2020 von https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit.html

Deutsches Bundesamt für Sicherheit in der Informationstechnik (2017), Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz.

Deutsches Bundesamt für Sicherheit in der Informationstechnik (2020), Kritische Infrastrukturen – Dokumente und Materialien. Abgerufen am 15.10.2020 von https://www.bsi.bund.de/DE/Themen/KI/Service/Material/dokumente_node.html#doc13085736bodyText5

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation (2017), Bericht - Zuständigkeiten im Bereich der Stromversorgungssicherheit.

Eidgenössische Elektrizitätskommission (2019), Bericht - Cyber-Sicherheit 2019.

Eidgenössische Elektrizitätskommission (2020), Marktüberwachung. Abgerufen am 19.11.2020 von https://www.elcom.admin.ch/elcom/de/home/themen/marktueberwachung.html

Eidgenössisches Finanzdepartement (2020) Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen - Rechtliche Grundlagen, S. 13.

Eidgenössische Finanzmarktaufsicht (2018), Jahresbericht 2018.

Eidgenössische Finanzmarktaufsicht (2019), Risikomonitor 2019.

Eidgenössische Finanzmarktaufsicht (2020a), Übersicht über die verschiedenen Bewilligungsformen. Abgerufen am 19.11.2020 von https://www.finma.ch/de/bewilligung/bewilligungsformen/

Eidgenössische Finanzmarktaufsicht (2020b), Aufsichtsmitteilung 05/2020 Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (2020), Betriebliche Datenschutzverantwortliche. Abgerufen am 19.11.2020 von https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/betriebliche-datenschutzverantwortliche/betriebliche-datenschutzverantwortliche.html

Energiegesetz (EnG) vom 30. September 2016 (Stand am 1. Januar 2018).

Electrosuisse (2019), Cybersecurity bei kleinen und mittleren Elektrizitätsversorgungsunternehmen.

Eidgenössisches Institut für Metrologie (2020), Konformitätsbewertungsstelle METAS-Cert. Abgerufen am 19.11.2020 von https://www.metas.ch/metas/de/home/dl/konformitaetsbewertungsstelle-metas-cert.html

Europäische Kommission (2016), Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie).

Europäische Kommission (2018), Rechtsakt zur Cybersicherheit.

Europäische Kommission (2019), Commission Recommendation on cybersecurity in the energy sector: C(2019) 2400 final.

Europäische Kommission (2020a), Proposal for directive on measures for high common level of cybersecurity across the Union.

Europäische Kommission (2020b), Public consultation to establish the priority list of network codes. Abgerufen am 19.11.2020 von https://ec.europa.eu/info/news/public-consultation-establish-priority-list-network-codes-2020-feb-11_lv

Europäische Kommission (2021), Summary Report on the open public consultation on the Directive on security of net-work and information systems (NIS Directive).

Energy Expert Cyber Security Platform (2017), Report - Cyber Security in the Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector.

European Network of Transmission System Operators for Electricity (2019), The Cyber Physical System for the Energy Transition. 2019. Digital Paper Executive Summary.pdf (entsoe.eu)

European Union Agency for Cybersecurity (2018), Report - Exploring the opportunities and limitations of current Threat Intelligence Platforms.

European Union Agency for Cybersecurity (2020), ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.

Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit (2018), Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit.

Luber, Stefan / Schmitz, Peter (2017), Definition SOC. Abgerufen am 19.11.2020 von https://www.security-insider.de/was-ist-ein-security-operations-center-soc-a-617980/

Luber, Stefan / Schmitz, Peter (2020), Definition SOAR. Abgerufen am 19.11.2020 von https://www.security-insider.de/was-ist-soar-a-933760/

Melde- und Analysestelle Informationssicherung (2020a), Social Engineering. Abgerufen am 16.11.2020 von https://www.melani.admin.ch/melani/de/home/themen/socialengineering.html

Melde- und Analysestelle Informationssicherung (2020b), Aktuelle Gefahren. Abgerufen am 16.11.2020 von https://www.melani.admin.ch/melani/de/home/themen.html

Nationales Zentrum für Cyber-Sicherheit (2020), Das Nationale Zentrum für Cybersicherheit. Abgerufen am 19.11.2020 von https://www.ncsc.admin.ch/melani/de/home/ueber_ncsc/das_ncsc.html

Postulat 17.3475 Graf-Litscher (2017), Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei Kritischen Infrastrukturen.

Schuster, Andreas (2021), Soll ich mein Unternehmen nach ISO 27001 zertifizieren?. Angerufen am 05.02.2021 von https://www.sec4you.com/warum-unternehmen-27001-zertifizieren/

Schweizerischen Akkreditierungsstelle (2020), Konformitätsbewertungsstellen. Abgerufen am 19.11.2020 von https://www.sas.admin.ch/sas/de/home.html

Smart Grids Task Force (2019), Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity – Final Report.

Stromversorgungsverordnung (StromVV) vom 14. März 2008 (Stand am 1. Januar 2020).

Swisspower (2019), Swisspower lanciert Kooperation für Cybersecurity in Stadtwerken. Abgerufen am 16.11.2020 von https://swisspower.ch/en/media/press-releases/swisspower-lanciert-kooperation-f%C3%BCr-cybersecurity-in-stadt-werken/

U.S. Department of Energy (2018), Cybersecurity Strategy 2018-2020.

Verband Schweizerischer Elektrizitätsunternehmen (2018a), Handbuch Grundschutz für Operational Technology.

Verband Schweizerischer Elektrizitätsunternehmen (2018b), Richtlinien für die Datensicherheit von intelligenten Messsystemen für Zertifizierung und Betrieb von intelligenten Messsysteme.

Verband Schweizerischer Elektrizitätsunternehmen (2018c), Standardisierter Datenaustausch für den Strommarkt Schweiz.

Verband Schweizerischer Elektrizitätsunternehmen (2019), Data Policy in der Energiebranche.

Zugehör, D. (2021) Hackerangriffe: Branche sucht Nähe zum BSI. Abgerufen am 04.02.2021 von https://www.energate-messenger.de/news/209373/hackerangriffe-branche-sucht-naehe-zum-bsi

Anhang 1: Detaillierte Auswertung der E-Survey

In dem Anhang werden die in Kapitel 3 vorgelegten Erkenntnisse der E-Survey begründet. Die Auswertung der Umfrage erfolgt entlang der folgenden vier Analysebereichen:

1. Modul 1: Aussagekräftigkeit der Umfrage

   Welche Unternehmen haben an der Erhebung teilgenommen? Wie ist die generelle Verteilung innerhalb der Teilnehmer und wie repräsentativ ist die E-Survey im Vergleich zum Gesamtmarkt Schweiz?

2. Modul 2: Aktuelles Maturitätsniveau der IT-Sicherheit im Stromsektor Schweiz

   Wie stehen alle Umfrage-Teilnehmer untereinander im Quervergleich betreffend Ihrer Maturität im Bereich der IT Sicherheit basierend auf den eigenen Angaben?

3. Modul 3: Aktuelles Maturitätsniveau der OT-Sicherheit im Stromsektor Schweiz

   Wie stehen alle Umfrage-Teilnehmer untereinander im Quervergleich betreffend Ihrer Maturität im Bereich der IT Sicherheit basierend auf den eigenen Angaben?

4. Modul 4: Weitere Erkenntnisse und Auffälligkeiten

   Welche weiterführenden Erkenntnisse konnten aus der Umfrage gezogen werden?

1.1 Analyse Modul 1: Aussagekraft der Umfrage

Die Umfrage wurde primär von Leiter der Unternehmensbereiche «IT» oder «Netzte» ausgefüllt. Rund 11% der Umfrage wurde von Leitern der Informationssicherheit, auch Chief Information Security Officer (CISO) genannt, beantwortet. Die Umfrage wurde zu 83% von deutschsprachigen Teilnehmern und zu 17% von französischsprechenden Teilnehmern ausgefüllt. Dies reflektiert die Sprache in welcher die Teilnehmer den Fragebogen ausgefüllt haben und nicht deren geographische Lage. In der Kommentarspalte war ersichtlich, dass auch italienischsprachige Personen an der Umfrage teilgenommen haben.

Die Unternehmen wurden weiter nach der Verteilung betreffend Anzahl dedizierte Mitarbeiter mit Verantwortung für IT- und/oder OT-Sicherheit befragt.[89] Wie Abbildung 25 zeigt, haben nur wenige der befragten Betriebe mehr als fünf dedizierte Mitarbeiter für IT- und/oder OT-Sicherheit. Indirekt gibt diese Beobachtung Aufschlüsse über die Grösse der Unternehmen. Vor allem bei den Unternehmen mit mehr als fünf dezidierten Mitarbeitern kann angenommen werden, dass es sich um relativ grosse Betriebe handelt. Jene Unternehmen, welche gar über zehn oder mehr spezialisierte Mitarbeiter verfügen, sind mit hoher Wahrscheinlichkeit marktdominante Energieunternehmen aufgrund ihrer Möglichkeit, monetär sowie organisatorisch, diese Mitarbeiter gezielt für den IT- oder OT-Sicherheitsbereich einstellen zu können.

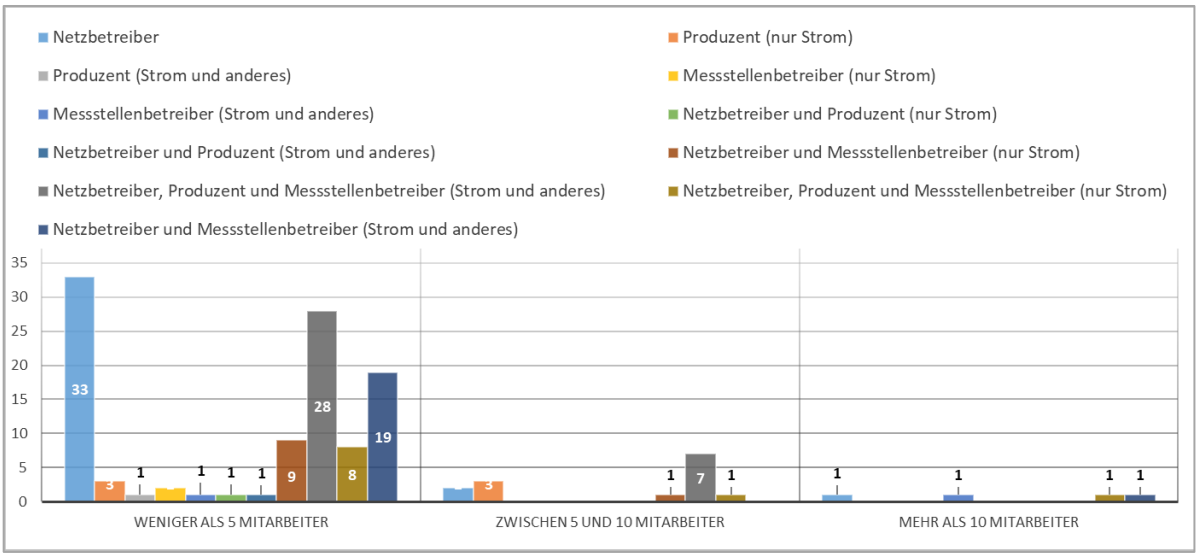


Abbildung 26: Dedizierte Mitarbeiter für IT/OT Sicherheit pro Unternehmertyp

89 Die Kategorisierung per Electrosuisse Umfrage «Cybersecurity bei kleinen und mittleren Elektrizitätsversorgungsunternehme» (2019) kann hier nicht direkt angewendet werden, da in der vorgängigen Umfrage die Gesamtzahl der Mitarbeiter und nicht jene mit spezifischem IT- oder OT-Sicherheits-Zuständigkeitsbereich berücksichtigt wurde.

Die Umfrageteilnehmer wurden auch gefragt, wer primär für Cyber-Sicherheit bei ihnen im Unternehmen verantwortlich ist. Abbildung 26 zeigt diese Verteilung. Vorwiegend ist die Verantwortung beim Leiter IT angesiedelt. Gefolgt vom Leiter Netz, dem CISO, sowie direkt dem oberen Kader (CEO, Vorstand). Der Kader war vermutlich vorrangig bei ganz kleinen Elektrizitätsunternehmen involviert. Interessanterweise wurden ebenfalls Dritte (Hersteller, externe Dienstleister) als Träger der Verantwortung angegeben. Dies ist insofern bemerkenswert, da eine Externalisierung der Verantwortlichkeit eine sehr hohe Abhängigkeit und eine unzureichende interne Rechenschaftspflicht für allfällige Cyber-Sicherheitsvorfälle bedeuten kann.

Rund ein Fünftel der Befragten gab zudem an, den Zuständigkeitsbereich für Cyber-Sicherheit innerhalb ihrer Unternehmung nicht genau definiert zu haben. Dies erscheint äusserst problematisch, da eine fehlende direkte Verantwortlichkeit für die Cyber-Sicherheit auf Mängel in wichtigen organisatorischen Strukturen und im Risikomanagement hinweisen kann. Es kann daraus gefolgert werden, dass bei etwa einem Viertel der Befragten, bei welchen entweder Dritte oder unbestimmte Personen für die Cyber-Sicherheit verantwortlich sind, mit hoher Wahrscheinlichkeit kein internes Informationssicherheits-Managementsystems (ISMS)[90] institutionalisiert wurde. Ein zentrales Element eines ISMS ist die Verankerung der Verantwortlichkeiten, damit die Sicherheitsprozesse entsprechend abgewickelt werden können. Ebenso sind die Risiken, welche im Rahmen des Risikomanagements im ISMS identifiziert werden, gewissen Stellen in den Unternehmen zuzuschreiben, um diese direkt an den Verantwortlichen zu binden und eine Rechenschaftspflicht zu kreieren. Da diese Verpflichtungen bei vielen nicht klar definiert sind, kann angenommen werden, dass Cyber-Risiken entsprechend nicht aktiv gemanagt werden.

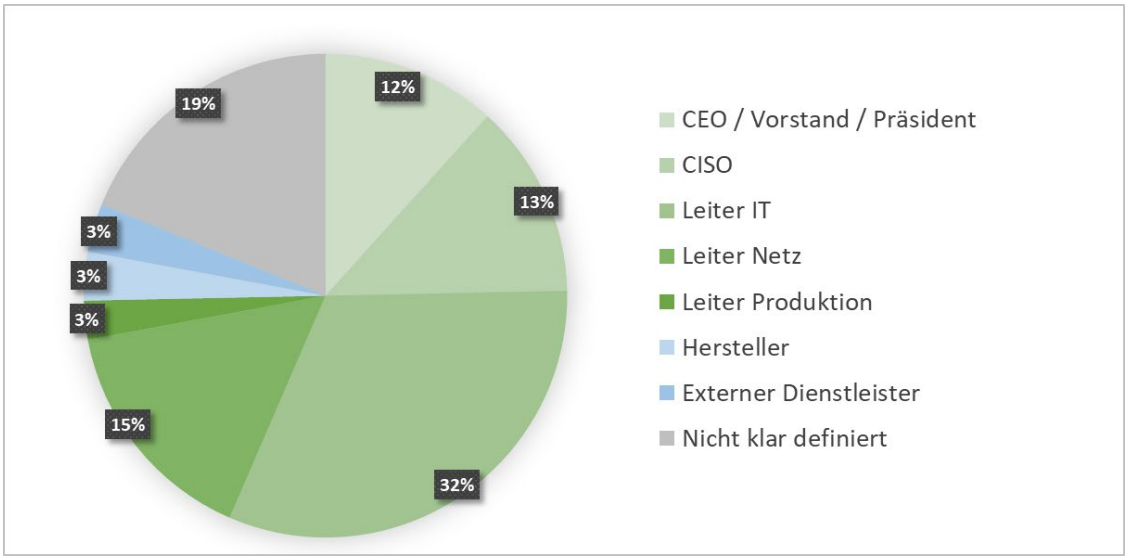


Abbildung 27: Verantwortlichkeit für Cyber-Sicherheit innerhalb der Unternehmen

[90] Unternehmensweit wirkendes Managementsystem, das die Einhaltung des Sicherheits- und Kontinuitätsniveaus von Informationen nachhaltig und effektiv sicherstellt.

Des Weiteren wurden alle Teilnehmer direkt gefragt, ob OT-Sicherheit heute in ihrer Unternehmung bereits adressiert und die damit verbundene Risiken aktiv verwaltet werden. 70% der 124 Teilnehmer gaben an, dass sich OT-Sicherheit aktuell bereits auf ihrer Unternehmensrisikolandkarte[91] befindet. Dies bedeutet, dass die Mehrheit der Teilnehmer versteht, dass die Informationssicherheit des eigenen Unternehmens zunehmend auch im Bereich der OT aktiv gemanagt werden sollte, und es nicht mehr genügt sich hierbei nur auf die hauseigene IT-Landschaft zu fokussieren. Es wird also erkannt, dass im Rahmen der zunehmenden Digitalisierung des Energiebereichs IT- und OT-Landschaft zunehmend verschmelzen. Durch technologische Entwicklungen wie z.B. in der 5G-Funkverbindung oder smarten Messgeräten, sind OT-Netze zunehmend nicht mehr physisch komplett abgeschottete Systeme und werden daher immer stärker und umfassender angreifbar. Eine künftig grössere Berücksichtigung der OT-Sicherheit auf der Risikolandkarte durch die Unternehmen ist daher unbedingt zu begrüssen.

Die Unternehmen wurden zudem gefragt, weshalb OT-Sicherheit mittlerweile in ihrer Unternehmung aktiv adressiert wird. Rund die Hälfte der Teilnehmer erklärte, dass das Thema OT-Sicherheit ursprünglich durch die interne und/oder externe Revision (Audit) als zusätzliches Unternehmens-Risiko aufgedeckt wurde, welches es künftig zu adressieren gilt. Unternehmen welche OT-Sicherheit aktuell noch nicht aktiv angehen haben sich auch überwiegend (48%) auch noch keine extensiven Gedanken dazu gemacht. Für den restlichen Teil war es eine reine Entscheidung des Managements ohne vorhergehende Revision die OT-Sicherheit aktiv zu managen. Nur ein Teilnehmer gab an, trotz Revision sich anschliessend bewusst dazu entschieden zu haben, Risiken im Bereich der OT-Sicherheit derzeit nicht aktiv im Unternehmen adressieren zu wollen.

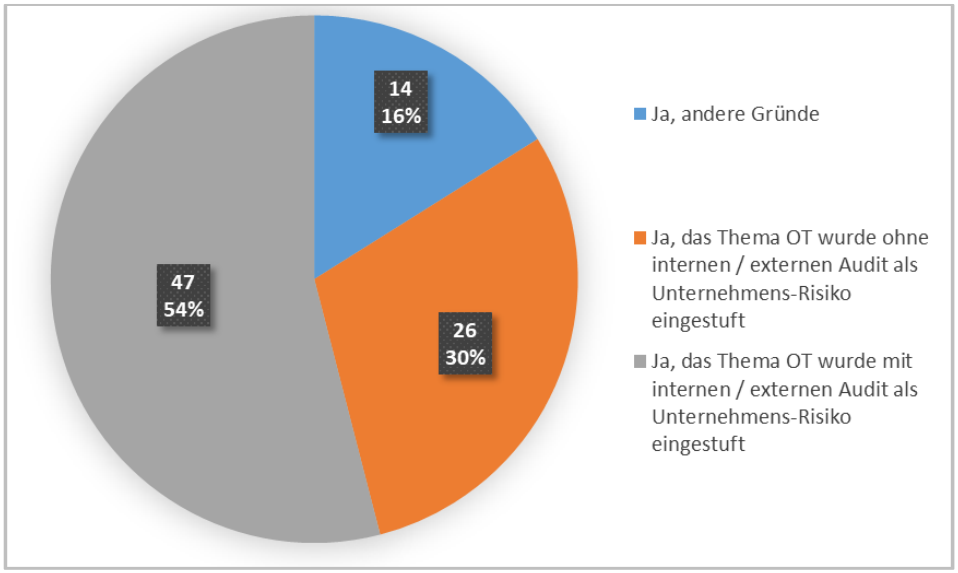


Abbildung 28: «Ja»-Begründungen für OT-Sicherheit auf Risikolandkarte

[91] Als wichtiger Bestandteil des Risikomanagements, fasst die Unternehmensrisikolandkarte die Risikoidentifikation und Risikobewertung eines Unternehmens zusammen. Das Management und die Fachbereiche sollten ihre Entscheidungen und Aktivitäten darauf ausrichten und anpassen um zu hohe Risiken zu vermeiden.

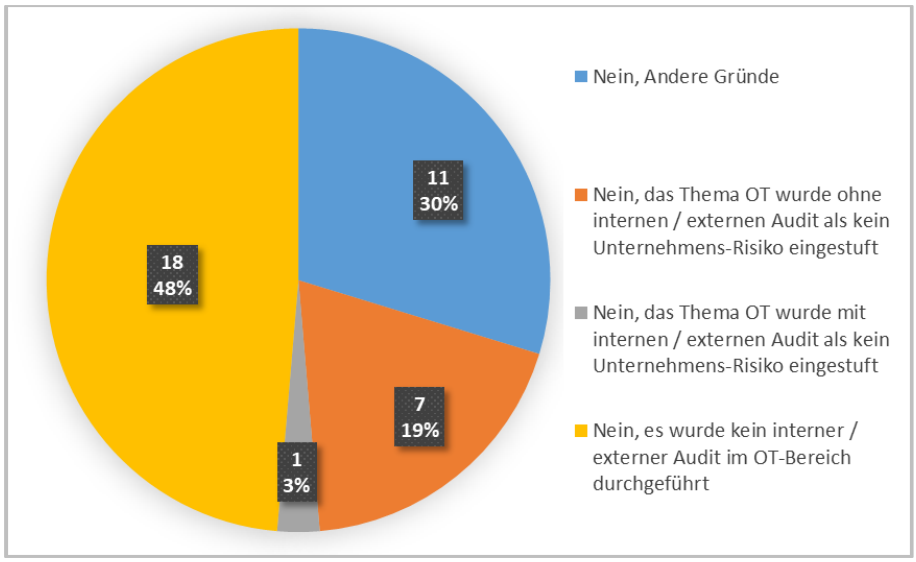


Abbildung 29: «Nein»-Begründungen für OT-Sicherheit auf Risikolandkarte

Repräsentation – Netzbetreiber

Von den 124 befragten Unternehmen, sind 113 in der Rolle als Netzbetreiber am Markt tätig. Dies entspricht, gemäss Angaben der ElCom, rund 18% der Gesamtmenge aller existierenden Netzbetreiber des Gesamtmarktes Schweiz im Jahr 2019. Dies ist eine in Bezug auf die Wichtigkeit des Themas und in Bezug zur Versorgungssicherheit eine verhältnismässig geringe Teilnahme. Die Begründung erscheint wenig trivial, ist doch Cyber-Sicherheit als ein wichtiges Ziel der Unternehmen und des Branchenverbandes deklariert worden. Zum einen wird es wohl daran liegen, dass die Teilnahme an der Umfrage freiwillig war. Anderseits könnte auch der Aufwand zur Beantwortung eine abschreckende Wirkung insbesondere bei kleinen und mittleren Unternehmen gezeigt haben, wobei dies wiederrum dahingehend verwundert, als dass lediglich eine bekannte Branchenrichtlinie abgefragt wurde. So muss beachtet werden, dass sich im Gesamtmarkt Schweiz auch eine grosse Anzahl an sehr kleinen Unternehmen in der Rolle als Netzbetreiber befindet.

Immerhin erreichen die in der Umfrage vertretenen 113 Netzbetreiber insgesamt eine beachtliche Stromeinspeisung von 43’318’662 MWh pro Jahr, welches 68% der jährlichen Gesamtstromeinspeisung aus den Kraftwerken in der Schweiz im Jahr 2019 entspricht (ohne die bereits ausgeklammerten Nuklearkraftwerke). In Anbetracht, dass nur eine geringe Teilnahmequote erreicht wurde, bedeutet dies, dass tendenziell grössere Netzbetreiber mit einer relativ hohen Stromeinspeisung den Fragebogen eingereicht haben.

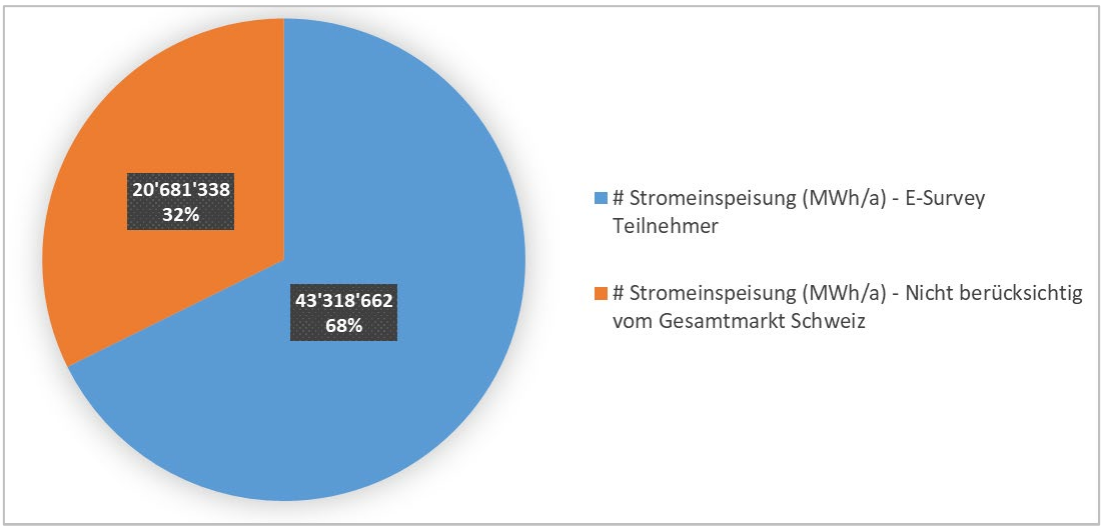


Abbildung 30: E-Survey Repräsentation - Stromeinspeisung Netzbetreiber (MWh/a)

Die Stromeinspeisung nach Unternehmenstyp gibt genaueren Einblick in das Zustandekommen der 68% der jährlichen Gesamtstromeinspeisung. Angesichts der vorherigen Bemerkung, dass die teilnehmenden Unternehmen nicht nur unter einem Unternehmenstyp agierten (also nur als Produzent oder Netzbetreiber oder Messstellenbetreiber), zeigt Abbildung 30 auf, dass die grosse Mehrheit der befragten Netzbetreiber gleichzeitig auch als Produzenten, sowie auch als Messstellenbetreiber für Strom und anderes tätig sind. Dies erhärtet die Annahme, dass viele der Umfrageteilnehmer grössere Betriebe repräsentieren, da sie diverse Angebote und Tätigkeitsbereiche am Markt realisieren.

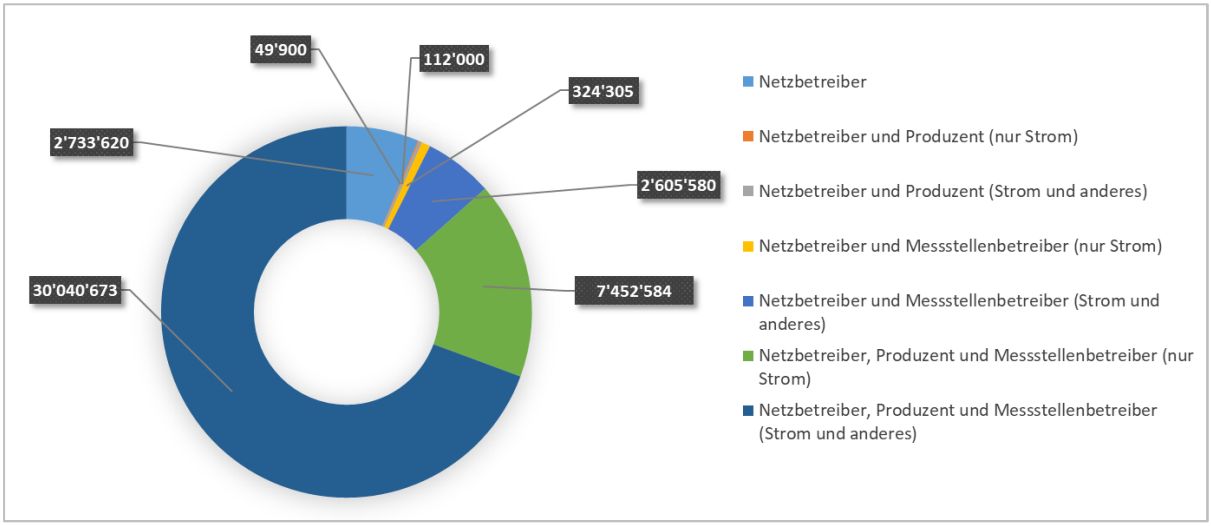


Abbildung 31: E-Survey Teilnahme - Netzbetreiber Stromeinspeisung nach Unternehmenstyp (MWh/a)

Von den 113 Netzbetreibern haben 93 Teilnehmer weiter spezifiziert, auf welchen Netzebenen sie operieren. Während viele Unternehmen gleichzeitig auf den beiden Netzebenen 5 und 7 vertreten sind, sind einzelne Unternehmen auf nur einer dieser beiden Ebenen tätig (Netzebene 5 oder Netzebene 7).

Wie zu erwarten sind bedeutend weniger Unternehmen auf den Netzebenen 1 und 3 vertreten, da grundsätzlich nur relativ wenig Betriebe auf diesen Ebenen agieren. So wird die Netzebene 1 in der

Schweiz ausschliesslich durch die Swissgrid betrieben, mit Ausnahme der Schaltfelder grösserer Kraftwerke, welche ebenfalls zur Netzebene 1 mitgezählt werden und durch die jeweiligen Produzenten betrieben werden.

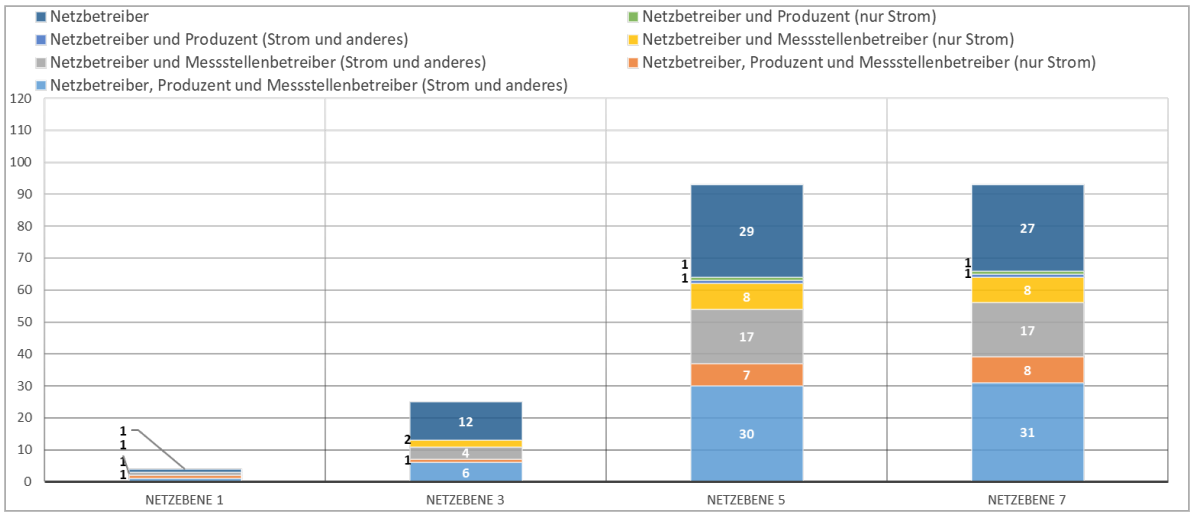


Abbildung 32: Netzbetreiber - Verteilung Netzebenen 1-7

Abbildung 32 zeigt, dass die Stromabgabe der 113 Netzbetreiber auf Netzebenen 4 und 5 relativ gleichmässig aufgeilt ist. Während nicht alle Netzbetreiber spezifizierten auf welchen Netzebenen sie operieren, haben hingegen alle ihre Stromabgabe per Netzebene aufgeführt. Rund ein Viertel gibt mehr als 25'000 MWh/a an, welches durch die Repräsentation grösserer Unternehmen erklärt ist. Abbildung 33, welche die Anzahl der Umfrageteilnehmer auf Netzebenen 4 und 5 mit der Gesamtzahl der Schweizer Netzbetreiber auf denselben Ebenen vergleicht, bestätigt die Annahme, dass tendenziell grössere Netzbetreiber an der Umfrage teilgenommen haben. Es sind aber dennoch genug Netzbetreiber mit einer geringeren Stromabgabe vertreten, um die Aussagekräftigkeit für den Schweizer Energiesektor zu bestätigen.

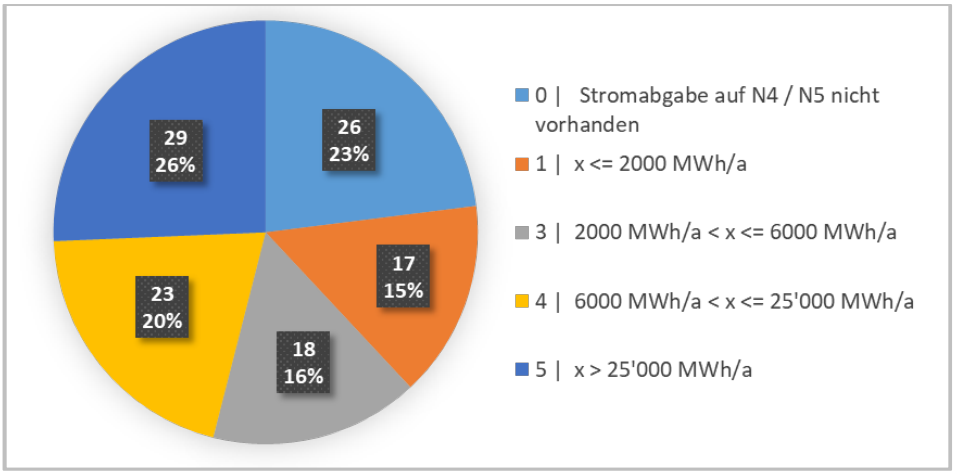


Abbildung 33: E-Survey Teilnahme - Stromabgabe der Netzbetreiber auf Netzebene 4 und 5 (MWh/a)

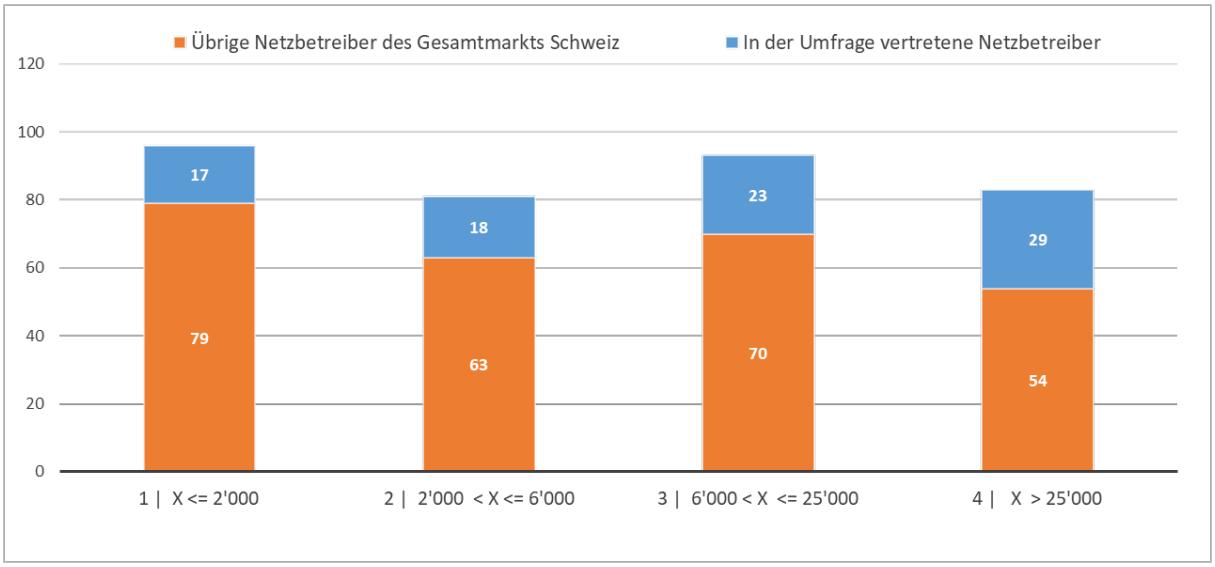


Abbildung 34: Stromabgabe der Netzbetreiber auf Netzebene 4 und 5 (MWh/a) - im Vergleich zum Gesamtmarkt Schweiz

Aus Abbildung 34 ergibt sich, dass auf Netzebene 6 und 7 vor allem Netzbetreiber zwischen 35'000 MWh/a und 220'000 MWh/a vertreten sind. Vergleicht man dies mit dem Gesamtmarkt Schweiz ist damit eine verhältnismässig starke Repräsentation von grossen Netzbetreibern der Netzebenen 6 und 7 gegeben.

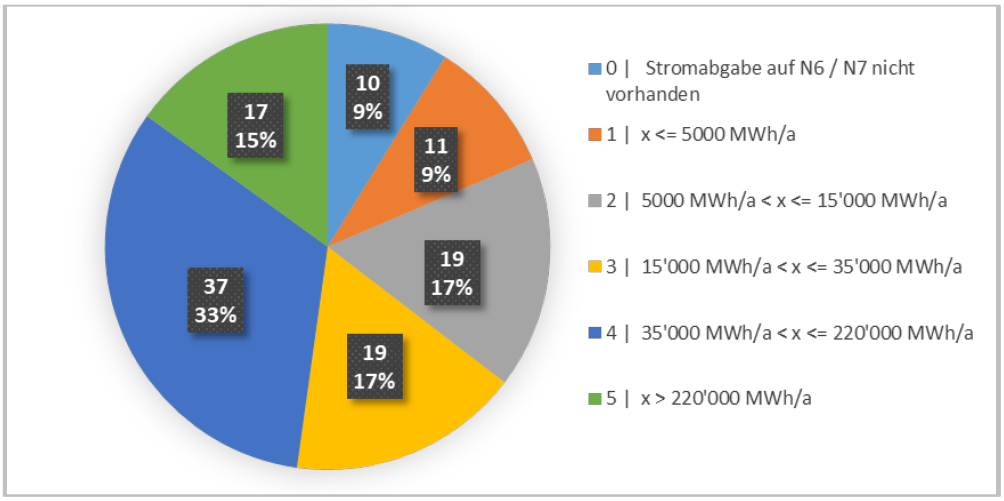


Abbildung 35: E-Survey Teilnahme - Stromabgabe der Netzbetreiber auf Netzebene 6 und 7 (MWh/a)

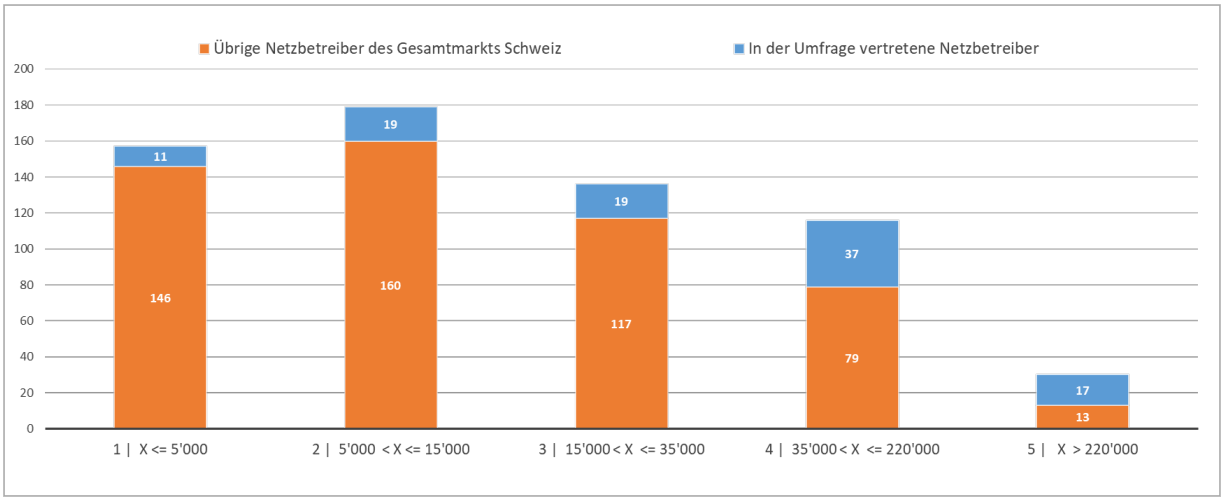


Abbildung 36: Stromabgabe der Netzbetreiber auf Netzebenen 6 und 7 (MWh/a) - im Vergleich zum Gesamtmarkt Schweiz

Abbilddung 36 zeigt die Gesamtnetzlänge auf Netzebene 5 (in km) von den in der Umfrage vertretenen 113 Netzbetreiber. Auf Netzebene 5 betreiben etwa ein Viertel der Betriebe zwischen 40km bis 300km. Vergleicht man dies mit dem Gesamtmarkt Schweiz ist abermals festzustellen, dass vor allem grössere Betriebe gut vertreten sind. Etwas mehr als die Hälfte dieser Betriebe haben an der Umfrage teilgenommen. Kleinere Netzbetreiber sind anzahlmässig gleich stark vertreten, repräsentieren aber prozentual einen kleineren Anteil innerhalb ihrer Gruppierung.

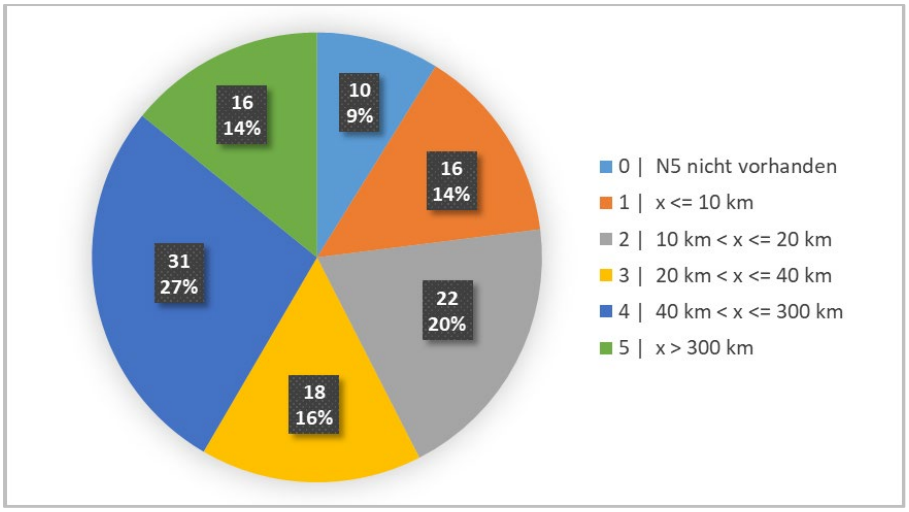


Abbildung 37: E-Survey Teilnahme – Gesamtlänge Netzbetreiber auf Netzebene 5 (km)

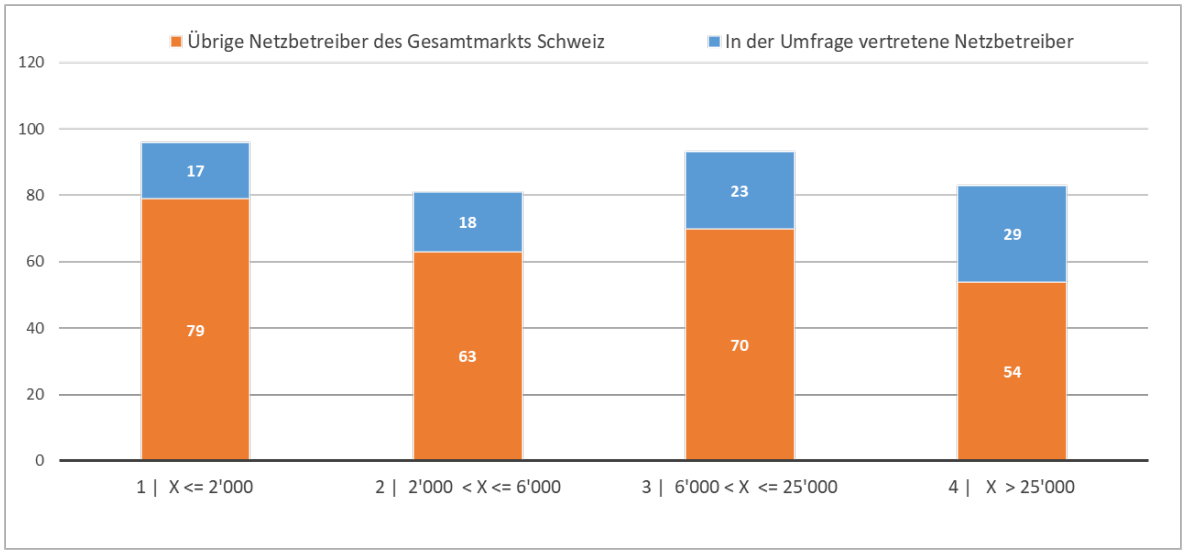


Abbildung 38: Gesamtlänge auf Netzebene 5 (km) - im Vergleich zum Gesamtmarkt Schweiz

Auf Netzebene 7 betrieben viele Unternehmen, 42%, eine Netzlänge zwischen 60km und 500km (vgl. Abbildung 38). Dies zeigt wiederholt auf, dass tendenziell eher grössere Betriebe an der Umfrage teilgenommen haben. Es ist dennoch ersichtlich, dass auch mittlere bis kleinere Unternehmen vertreten sind, da tiefere Netzlängen ebenfalls vorhanden sind.

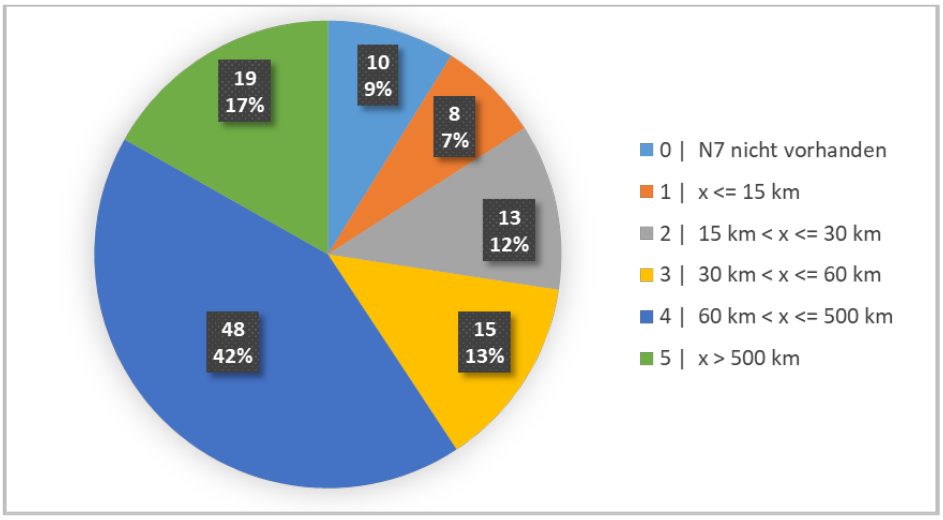


Abbildung 39: E-Survey Teilnahme - Gesamtlänge auf Netzebene 7 (km)

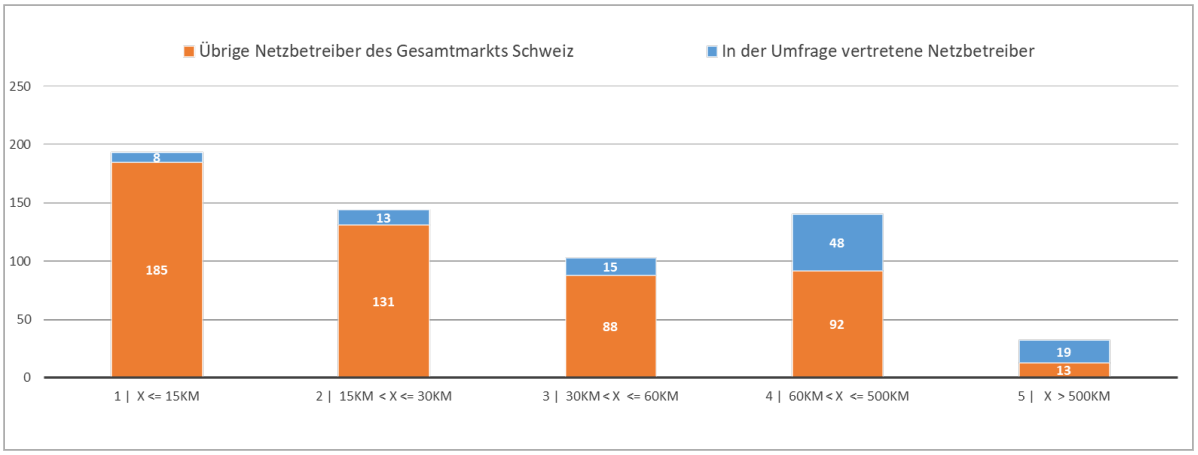


Abbildung 40: Gesamtlänge auf Netzebene 7 (km) - im Vergleich zum Gesamtmarkt Schweiz

Repräsentation – Produzenten

Es wurden alle Produzenten des Gesamtmarktes Schweiz im Jahr 2019 mit einer Stromproduktion von >5MGh/a (ohne Atom) angefragt. 54 Produzenten, also 50% aller Stromproduzenten, welche durch das BFE für die Umfrage angefragt wurden, nahmen daran teil. Es ist jedoch anzumerken, dass es keine vollständige Liste der Produzenten in der Schweiz gibt. Die in der Umfrage vertretenen 54 Produzenten erreichen insgesamt eine Stromproduktion von 18'245'244 MWh/a, welches ungefähr 43% der jährlichen Gesamtproduktion 2019 ohne die Nuklearkraftwerke in der Schweiz entspricht.

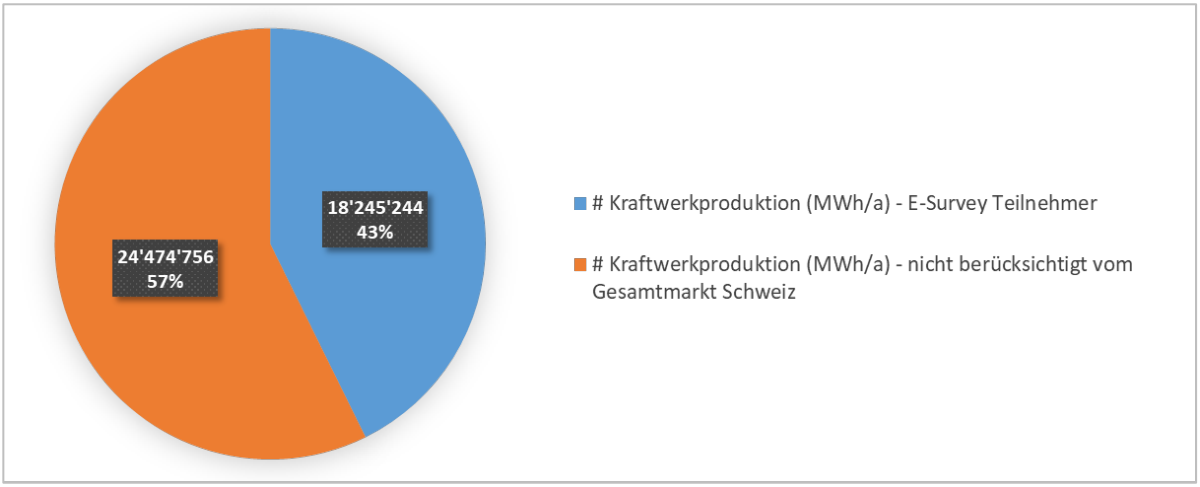


Abbildung 41: E-Survey Repräsentation - Kraftwerkproduktion (MWh/a - ohne Atomstrom)

De Verteilung bezüglich dem spezifischeren Unternehmenstyp der Produzenten in Abbildung 41 zeigt auf, dass reine «Produzenten (nur Strom)» und integrierte Unternehmen welche «Netzbetreiber, Produzent und Messstellenbetreiber (Strom und anderes)» umfassen, etwa gleichmässig vertreten sind. «Netzbetreiber, Produzent und Messstellenbetreiber (nur Strom)» stellen den drittgrössten Unternehmenstyp gemessen an der Stromproduktion nach Unternehmenstyp dar.

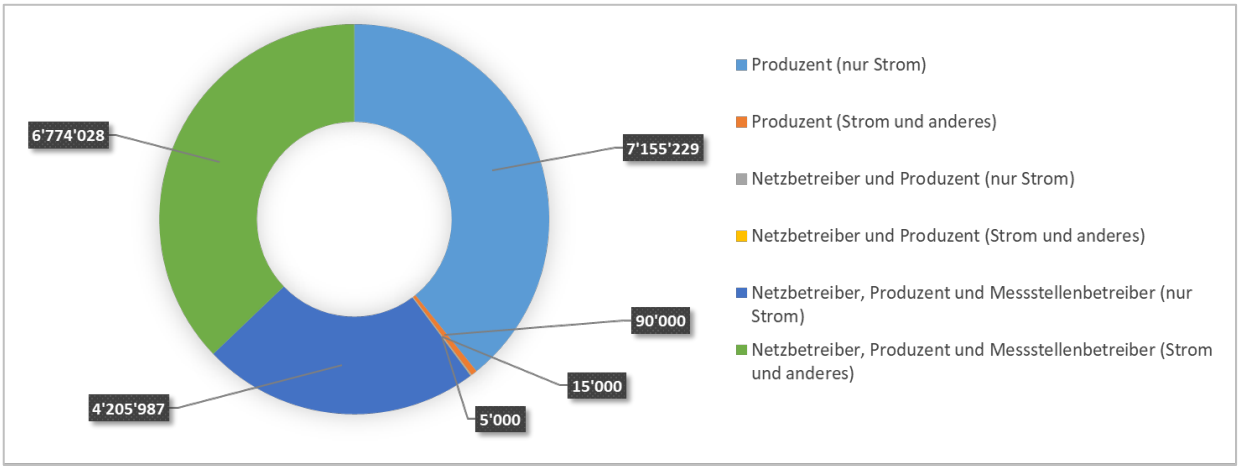


Abbildung 42: E-Survey Teilnahme - Stromproduktion nach Unternehmenstyp (MWh/a)

Die in der Umfrage vertretenen 54 Produzenten haben 52 Teilnehmer weiter spezifiziert, auf welchen Netzebenen sie operieren. Es zeigt sich hierbei eine sehr ähnliche Verteilung wie bei den Netzbetreibern, das heisst der Grossteil der Unternehmen ist auf den Ebenen 4 und 5 oder Ebenen 6 und 7 zu finden. Die Produzenten auf Netzebene 1 sind Betreiber grosser Kraftwerke, dessen Schaltfelder ebenfalls zur Netzebene 1 mitgezählt werden.

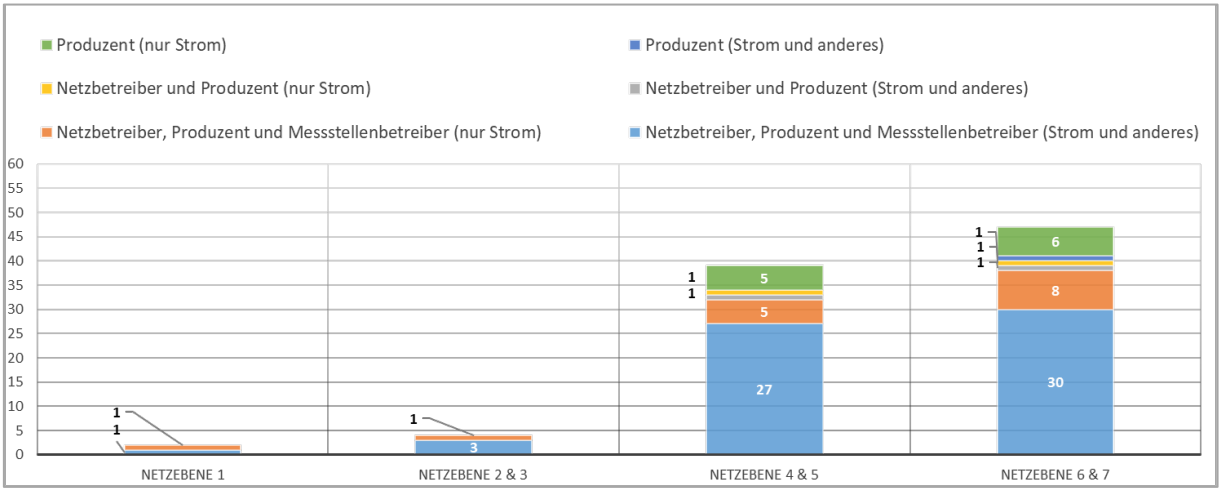


Abbildung 43: Produzenten - Verteilung Netzebenen 1-7

Repräsentation – Messstellenbetreiber

Die in der Umfrage teilnehmenden 79 Messstellenbetreiber decken gemeinsam insgesamt 2‘257‘125 Messpunkte ab. Dies entspricht, gemäss Angaben der ElCom, ungefähr 40% aller existierenden Messpunkte in der Schweiz im Jahr 2019. Es ist jedoch hinzuzufügen, dass alle bekannten Unternehmen angefragt wurden, es jedoch keine vollständige Liste der Messstellenbetreiber in der Schweiz gibt. Der grösste Anteil der Befragten, 72%, sind zudem auch der Gruppe der integrierten Unternehmen mit Netzbetrieb und Produktion zuzuteilen.

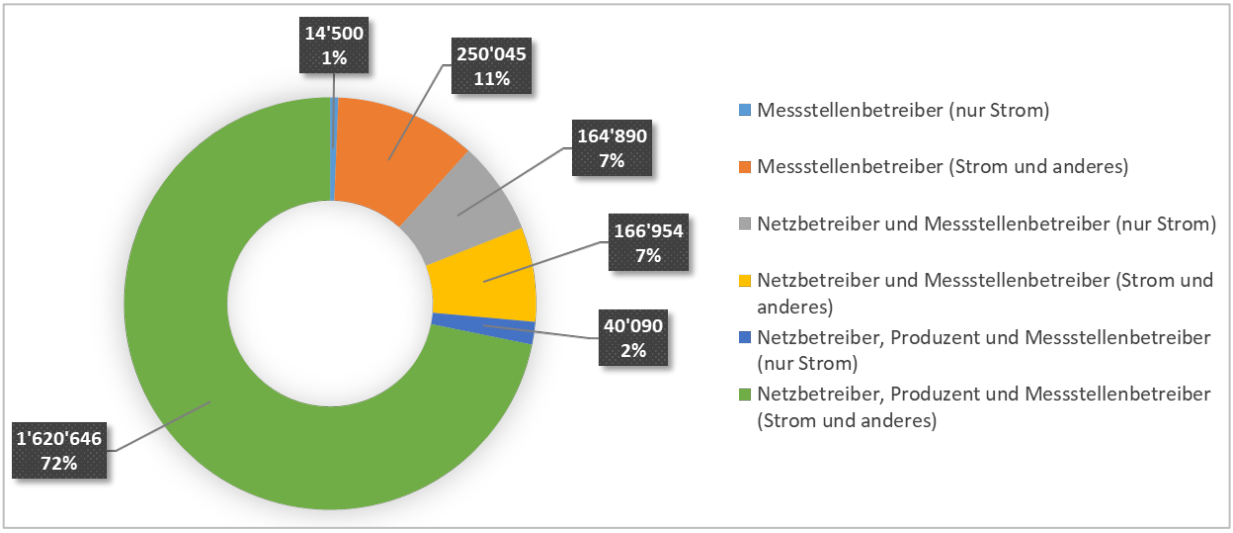


Abbildung 44: E-Survey Teilnahme - # Messpunkte nach Unternehmenstyp

1.2 Analyse Modul 2 & 3: aktuelles IT-/OT-Maturitätsniveau

Die nachfolgenden Beobachtungen bezüglich den Stärken und Schwächen im Maturitätsniveau der Unternehmen der Elektrizitätswirtschaft zu IT und OT sind essentielle Indikatoren, um später systemische Lösungsansätze für Cyber-Sicherheit und Cyber-Resilienz entwickeln zu können. Dieser Umfrageteil wurde entlang dem IKT Minimalstandard des BWL bzw. teilweise dem OT Grundschutz des VSE aufgebaut. Alle Umfrageteilnehmer wurden beauftragt, ihre eigene Maturität betreffend IT- und OT- Sicherheit entlang der fünf Funktionen und 23 Unterkategorien (= Cyber-Fähigkeiten) des Standards selbst einzuschätzen.

Der Fragebogen folgt dem IKT Minimalstandard in dem Aufbau der Fragen und besteht aus fünf Funktionen mit insgesamt 23 Unterkategorien. Nachfolgend werden diese Kategorien und Unterkategorien aufgeführt, weil die Umfrageteilnehmer entlang dieser Unterkategorien befragt wurden:

Identifizieren: befasst sich mit der Entwicklung für das organisatorische Verständnis des eigenen Unternehmens.

- Inventar Management: Die Daten, Personen, Geräte, Systeme und Anlagen einer Organisation sind identifiziert, katalogisiert und bewertet. Die Bewertung soll ihrer Kritikalität hinsichtlich der zu erfüllenden Geschäftsprozesse sowie der Risikostrategie der Organisation entsprechen.
- Geschäftsumfeld: Die Ziele, Aufgaben und Aktivitäten des Unternehmens sind priorisiert und bewertet. Diese Informationen dienen als Grundlage für die Zuweisung der Verantwortlichkeiten.
- Vorgaben (Governance): Die Governance regelt Zuständigkeiten, überwacht und stellt sicher, dass regulatorische, rechtliche und operationelle Anforderungen aus dem Geschäftsumfeld eingehalten werden.
- Risikoanalyse: Die Organisation kennt die Auswirkungen von Cyber-Risiken auf die Geschäftstätigkeit, auf Betriebsmittel und Individuen, inklusive Reputationsrisiken.
- Risikomanagementstrategie: Die Prioritäten, Einschränkungen und maximal tragbaren Risiken Ihrer Organisation sind festzulegen, sowie die operativen Risiken auf dieser Grundlage zu bewerten.
- Lieferketten-Risikomanagement: Die Prioritäten, Einschränkungen und maximalen Risiken sind der Organisation in Zusammenhang mit Lieferantenrisiken sind festzulegen.

Schützen: unterstützt die Fähigkeit zur Verhinderung von Cyber-Sicherheitsvorfällen.

- Zugriffsmanagement und –steuerung: Der physische und logische Zugriff auf IKT-Betriebsmittel und –Anlagen ist nur für autorisierte Personen, Prozesse und Geräte möglich, und der Zugriff soll nur für zulässige Aktivitäten möglich sein.
- Sensibilisierung und Ausbildung: Die Mitarbeitenden und externen Partner sind regelmässig bezüglich aller Belange der Cyber-Sicherheit angemessen zu schulen und auszubilden.
- Datensicherheit: Informationen, Daten und Datenträger sind so zu managen, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gemäss der Risikostrategie der Organisation geschützt werden.
- Informationsschutzrichtlinien: Richtlinien zum Schutz von Informationssystemen und Betriebsmitteln sind zu erstellen.
- Unterhalt: Die Unterhalts- und Reparaturarbeiten an Komponenten des IKT-Systems und/oder des Industrial Control System (ICS) sind gemäss den geltenden Richtlinien und Prozessen durchzuführen.

- Einsatz von Schutztechnologie: Technische Security-Lösungen sind zu installieren, um die Sicherheit und Resilienz Ihrer IKT-Systeme und Ihrer Daten gemäss den Vorgaben und Prozessen zu garantieren.

Erkennen: diese Funktion bietet einen relativ neuen Blickwinkel auf die Informationssicherheit und ergänzt die traditionellen Sicherheitsziele auf die Identifikation eines möglichen Vorfalls. Erfahrungen haben gezeigt, dass Unternehmen heutzutage davon ausgehen müssen bereits Ziel eines – meist erfolgreichen – Angriffs geworden zu sein oder in der Zukunft zu werden und deshalb wird diese Funktion zunehmend wichtiger.

- Auffälligkeiten und Vorfälle: Auffälligkeiten (abnormes Verhalten) und sicherheitsrelevante Ereignisse sind zeitgerecht zu erkennend und potenzielle Auswirkungen des Vorfalls müssen verstanden werden.
- Überwachung: Das IKT-System inkl. aller Betriebsmittel, ist in regelmässigen Intervallen zu überwachen, um einerseits Cyber-Sicherheitsvorfälle zu entdecken und anderseits die Effektivität der Schutzmassnahmen überprüfen zu können.
- Detektionsprozess: Prozesse und Handlungsanweisungen zur Detektion von Cyber-Sicherheitsvorfällen werden gepflegt, getestet und unterhalten.

Reagieren: wird eine Cyberattacke einmal erkannt zielt diese Funktion darauf ab, diese möglichst schnell und effizient bekämpfen zu können.

- Reaktionsplanung: Ein Reaktionsplan zur Adressierung erkannter Cyber-Sicherheitsvorfälle ist aufzustellen.
- Kommunikation: Reaktionsprozesse mit den internen und externen Anspruchsgruppen sind abgestimmt.
- Analyse: Regelmässig Analysen sind durchzuführen, um eine adäquate Reaktion auf Cyber-Sicherheitsvorfälle zu ermöglichen.
- Schadensmeldung: Eine weitere Ausbreitung eines Cyber-Sicherheitsvorfalls ist zu verhindern.
- Verbesserungen: Die Reaktionsfähigkeit der Organisation auf eingetretene Cyber-Sicherheitsvorfälle soll laufend verbessert werden, indem die Lehren aus vorangegangenen Vorfällen gezogen werden.

Wiederherstellen: nach einer Attacke müssen betroffene Systeme wiederhergestellt werden sowie kontinuierliche Verbesserungsprozesse dürfen nicht vernachlässigt werden.

- Wiederherstellungsplanung: Wiederherstellungsprozesse müssen so gepflegt und durchgeführt werden, dass eine zeitnahe Wiederherstellung der Systeme gewährleistet werden kann.
- Verbesserungen: Die Wiederherstellungsprozesse werden laufend verbessert, indem Lehren aus vorangegangenen Wiederherstellungen gezogen werden.
- Kommunikation: Wiederherstellungsaktivitäten mit internen und externen Partnern, z.B. Internet Service Providern, Behörden, Systemintegratoren etc, sind sicherzustellen.

Um das Niveau der teilnehmenden Unternehmen betreffend IT- und OT-Sicherheitsmaturität jeweils voneinander getrennt erfassen zu können, wurde die Fragen zum Maturitätsniveau in zwei Module aufgeteilt. Für eine Selbsteinschätzung betreffend Maturität der IT-Sicherheit, wurden alle 23 Unterkategorien (= Cyber-Fähigkeiten) des IKT Standards einzeln in Modul 2 abgefragt. Hingegen wurden für die Einschätzung der OT-Sicherheit nur gewisse Unterkategorien abgefragt, welche aus Sicht der Umfrageersteller darauf zutreffen. Dem ist so, da gewisse Cyber-Fähigkeiten (= Unterkategorien) prinzipiell

für die gesamte Unternehmung gelten und nicht nochmals spezifisch aus einer OT-Sicherheitsbetrachtung abgefragt werden müssen. Das bedeutet, dass in der Analyse in Modul 2 betreffend IT-Sicherheit alle Unterkategorien vorhanden sind, wogegen in bei der Analyse in Module 3 betreffend OT-Sicherheit nicht alle Unterkategorien erklärt sind, da diese die gleichen Cyber-Fähigkeiten wie die IT-Sicherheit berühren und daher schon in dem Bereich der IT-Sicherheit beinhaltet sind.

Wie bereits ausgelegt, wurden die Umfrageteilnehmer gefragt, gemäss 'IKT Minimalstandard' die eigene Maturität pro Unterkategorie in eine von fünf Maturitätsstufen ('Levels') selbst einzuschätzen.[92] Es wurden keine weiterführenden Kriterien für die (Nicht-)Erfüllung der Maturitätsstufen für die jeweiligen Unterkategorien angegeben und da auch keine Nachweise angefordert wurden ist die Subjektivität der Einschätzungen abermals hervorzuheben.

Maturitätsstufe 0: Nicht Umgesetzt»

Maturitätsstufe 1: Partiell umgesetzt, nicht vollständig definiert und abgenommen:

- Risikomanagementprozesse und organisatorische Vorgaben zur IKT-Sicherheit sind nicht formalisiert, und die IKT-Risiken werden üblicherweise nur ad hoc oder reaktiv verwaltet.
- Ein integriertes Risikomanagementprogramm auf organisatorischer Ebene besteht, aber ein Bewusstsein für IKT-Risiken und ein organisationsweiter Ansatz zur Bewältigung dieser Risiken sind nicht etabliert.
- Die Organisation verfügt typischerweise nicht über Prozesse, um Informationen zur Cybersecurity innerhalb der Organisation gemeinsam zu nutzen.
- Ebenso verfügt die Organisation für den Fall eingetretener IKT-Risiken oft nicht über standardisierte Prozesse zum Informationsaustausch oder zur koordinierten Zusammenarbeit mit externen Partnern.

Maturitätsstufe 2: Partiell umgesetzt, vollständig definiert und abgenommen:

- Organisationen, die sich selber auf dem Tier Level 2 einordnen, verfügen typischerweise über Risikomanagementprozesse für IKT-Risiken. Diese sind jedoch nicht als konkrete Handlungsanweisungen implementiert.
- Auf der organisatorischen Ebene sind IKT-Risiken ins unternehmensweite Risikomanagement integriert, und das Bewusstsein für IKT-Risiken ist auf allen Unternehmensstufen vorhanden.
- Hingegen fehlen typischerweise unternehmensweite Ansätze zur Steuerung und Verbesserung des Bewusstseins (Awareness) für aktuelle und zukünftige IKT-Risiken. Genehmigte Prozesse und Verfahren sind definiert und umgesetzt.
- Das Personal verfügt über ausreichende Ressourcen, um seine Aufgaben im Bereich der Cybersecurity wahrzunehmen.
- Cyber-Security-Informationen werden innerhalb der Organisation auf informeller Basis geteilt.
- Die Organisation ist sich ihrer Rolle bewusst und kommuniziert mit externen Partnern zum Thema Cybersecurity (z.B. Kunden, etc.).
- Es bestehen jedoch keine standardisierten Prozesse zur Kooperation oder zum Informationsaustausch mit diesen Partnern.

---

[92] Die unabhängige Electrosuisse Umfrage verwendete die gleiche Struktur sowie Maturitätsstufen entlang des IKT Minimalstandards, aber war begrenzt auf die Befragung von kleinen und mittleren Elektrizitätsversorgungsunternehmen bzw. den Produzenten.

Maturitätsstufe 3: Umgesetzt, vollständig oder grösstenteils umgesetzt, statisch:

- Verfügen über formell genehmigte Risikomanagementpläne und Vorgaben zu deren unternehmensweiten Anwendung.
- Der Umgang mit IKT-Risiken ist in unternehmensweit gültigen Richtlinien definiert.
- Die standardisiert erfassten IKT-Risiken sowie die Vorgaben zum Umgang mit denselben werden regelmässig aktualisiert.
- Dabei werden sowohl Veränderungen der Geschäftsanforderungen berücksichtigt als auch technische Weiterentwicklungen und eine sich verändernde Bedrohungslandschaft, etwa durch neue Akteure oder ein sich wandelndes politisches Umfeld. Prozesse und Verfahren zum Umgang mit veränderten Risiken sind schriftlich definiert.
- Das Personal verfügt über die notwendigen Kenntnisse und Fähigkeiten, um seine Aufgaben zu erfüllen.
- Die Organisation kennt ihre Abhängigkeiten von externen Partnern und tauscht mit diesen Informationen aus, die Managemententscheidungen innerhalb der Organisation als Reaktion auf Vorfälle ermöglichen.

Maturitätsstufe 4: Dynamisch, umgesetzt, kontinuierlich überprüft, verbessert:

- Organisation alle Anforderungen aus den Tier Leveln 1–3 vollständig erfüllt und zusätzlich die eigenen Prozesse, Methoden und Fähigkeiten ständig überprüft und bei Bedarf verbessert.
- Grundlage zur kontinuierlichen Verbesserung ist eine lückenlose Dokumentation sämtlicher Cybersecurity-Vorfälle.
- Die Organisation zieht die notwendigen Lehren aus der Analyse vergangener Vorfälle und passt die eigenen Prozesse und eingesetzten Sicherheitstechnologien dynamisch dem neusten Stand der Technik oder sich wandelnden Bedrohungslagen an. IKT-Risikomanagement ist fester Bestandteil der Unternehmenskultur.
- Erkenntnisse aus vergangenen Vorfällen, Informationen von externen Quellen und aus der permanenten Überwachung der eigenen Systeme und Netzwerke werden fortwährend in den Risikomanagementprozess integriert.
- Die Organisation teilt laufend Informationen mit Partnern und verfügt dazu über standardisierte Prozesse.

Kommentar zu Unternehmenstypen: Wie bereits erklärt, wurde die Maturität entlang fünf Unternehmenstypen ausgewertet, nämlich «Netzbetreiber», «Produzent – nur Strom», «Produzent – Strom und anderes», «Messstellenbetreiber – nur Strom» und «Messstellenbetreiber – Strom und anderes». Dies bedeutet, dass einige Unternehmen doppelt oder gar dreifach in diesen fünf Unternehmenskategorien für die Durchschnittswerte vertreten sein können.

In der nachfolgenden Analyse wurden die fünf Funktionen entlang ihrer spezifischen Unterkategorien getrennt um die jeweilige Maturität der IT-Sicherheit in den verschiedenen Cyber-Fähigkeitsbereichen genauer untersuchen zu können.

1.2.1 Auswertung Modul 2: aktuelles IT- Maturitätsniveau

In Kapitel 3 wurde eine Gesamtübersicht über die fünf IKT Minimalstandard Funktionen dargelegt (vgl. Abbildung 9). In diesem Kapitel werden die einzelnen Kategorien genauer analysiert und entlang den 23 Cyber-Fähigkeiten bezüglich der IT-Sicherheit ausgewertet.

Innerhalb der **IT-Kategorie «Identifizieren»** sticht insbesondere eine allgemeine Schwäche im Bereich des Lieferketten-Risikomanagements, auch als «Third Party Risk Management» bekannt, ins Auge. Die Umfrageteilnehmer befinden ziemlich genau zwischen den Maturitätswerten 0 und 1, welches vergleichsweise besonders tief ist. Diesbezüglich darf erklärend angenommen werden, dass tendenziell wohl zuerst interne Prozesse geregelt wurden und erst später externe Anbieter überprüft werden. Die Umfrageteilnehmer vertrauen der Cyber-Sicherheit ihrer Lieferanten offenbar meist ohne fundierte Nachweispflichten oder Leistungsspezifikationen, trotz den erheblichen Risiken, welche mit der grossen direkten oder auch indirekten Abhängigkeit verbunden sind. Eine einmalige, initiale Überprüfung von Lieferanten genügt zudem nicht, da die sicherheitsrelevanten Komponenten in den Produkt- und Dienstlebenszyklus integriert sein, sowie auch systematisch verwaltet werden müssen. Diese Unterkategorie ist ein zentraler Bestandteil eines internen ISMS und die Vermutung scheint sich hier zu erhärten, dass dieses Managementsystem noch nicht in allen Unternehmen genügend institutionalisiert wurde und entsprechende Cyber-Risiken nicht verwaltet werden.

Des Weiteren, zeigen die anderen beiden Bereiche des Risikomanagements auch relativ tiefe Maturitätswerte auf. Sie liegen im Schnitt unter dem Maturitätsniveau 1, welches «partiell umgesetzt, nicht vollständig definiert und abgenommen» bedeutet. Offenbar sind Prioritäten und Einschränkungen für maximal tragbare IT-Sicherheitsrisiken nicht geklärt oder kommuniziert und die Auswirkungen möglicher Cyber-Risiken nicht bekannt. Diese Vermutung wird durch die Ergebnisse der ElCom Umfrage insbesondere für solche Unternehmen welche, teils unter Anderem, als Netzbetreiber agieren zusätzlich unterstützt. Diese haben in der ElCom Umfrage angegeben, dass das Thema IT Sicherheits-Risikomanagement und Lieferketten Risikomanagement betreffend Informationssicherheit lediglich nach Bedarf, also auf einer ad-hoc Basis, in der Geschäftsleitung thematisiert werden.[93] Hingegen scheinen die Bereiche «Governance» und «Inventar Management» am solidesten in den Unternehmen verankert zu sein.

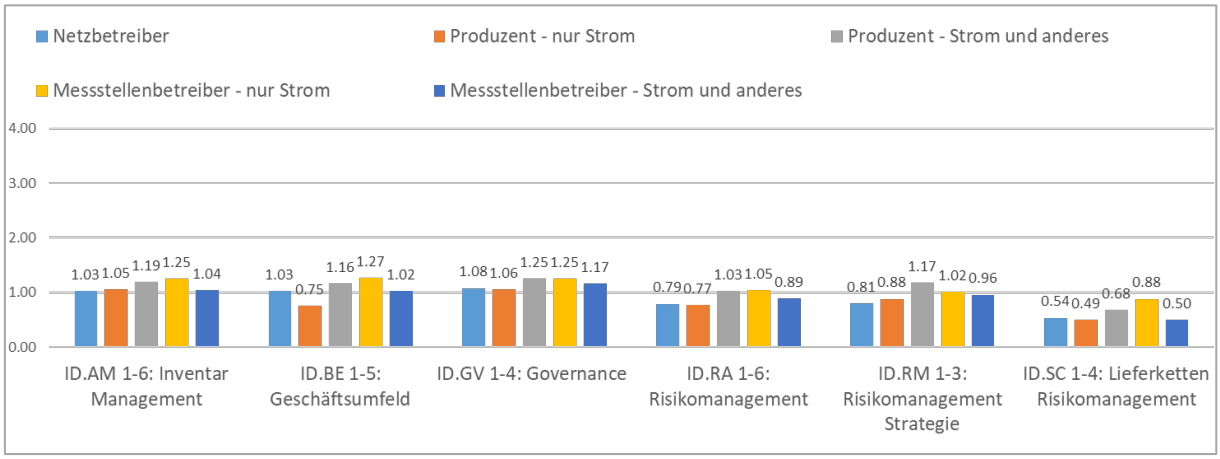


Abbildung 45: Maturität IT-Kategorie «Identifizieren»

[93] Eidgenössische Elektrizitätskommission (2019), Bericht - Cyber-Sicherheit 2019.

Innerhalb der **IT-Kategorie «Schützen»** scheinen die meisten Umfrage-Teilnehmer in den Bereichen «Zugriffsmanagement und -steuerung», sowie «Awareness & Training» bereits fortgeschrittener als die anderen Cyber-Fähigkeiten zu sein, da die beiden Unterkategorien sich klar über der Maturitätsstufe 1 befinden. Dies bedeutet, dass zumindest gewisse Basiskenntnisse in diesen Bereichen bestehen. Insbesondere das Zugriffsmanagement und die -steuerung erreichen ein verhältnismässig gutes Maturitätsniveau, welches sicherstellt, dass der physische, sowie logische Zugriff auf den IT-Bereich nur für autorisierte Personen, Prozesse und Geräte möglich ist. Die Schulung und Sensibilisierung einzelner Mitarbeiter ist beutend, da bei der Cyber-Sicherheit durch sogenanntes «Social Engineering»[94] der Mensch oft als eine zentrale Schwachstelle für Cyber-Attacken ausgenutzt wird. Ein typisches Szenario ist z.B. das Anklicken eines Links in einer E-Mail womit versucht wird Malware[95] zu installieren. Aber auch der Austausch von Daten über nicht autorisierte Mail- oder Clouddienste kommt öfters vor. Trainings sind daher wichtig um den Mitarbeitern ein Bewusstsein für Sicherheitsthemen zu institutionalisieren und das entsprechende Verhalten zu verbessern, damit diese nicht absichtlich oder unabsichtlich einen Cyber-Vorfall auslösen. Die Schulung von externen Partnern muss ebenso überprüft werden, damit diese ihre sicherheitsrelevanten Aufgaben gemäss den zugehörigen Vorgaben und Prozessen ausführen können. Aufgrund der oben festgestellten Schwäche der Umfrageteilnehmer bei dem IT-Lieferkennten Risikomanagement ist aber anzunehmen, dass dies wahrscheinlich bei den Betrieben nicht berücksichtigt wird.

Die Bereiche Datenschutz und technische Schutzmassnahmen zeigen ebenfalls noch Verbesserungsbedarf auf, damit diese über die rudimentäre Basisstufe 1 wachsen können. Daten müssen vor Verletzungen der Vertraulichkeit, der Integrität und der Verfügbarkeit geschützt werden. Es müssen zudem Richtlinien erlassen werden, um Informationssysteme und Betriebsmittel zu schützen, damit der Datenschutz garantiert werden kann.

Der Stand bei technischen Massnahmen wie «Maintenance» und «Protective Technology» überzeugt bisher ebenfalls nicht und suggeriert, wie auch schon die anderen Kategorien einen Weiterentwicklungsbedarf. Sie sind nicht nur die Durchführung der Installation von technischen Security-Lösungen und deren Unterhalts- und Reparaturarbeiten kritisch, sondern auch deren Aufzeichnung und Dokumentation (Logging), um allfällige wichtige Rückschlüsse bei einem Cyber-Sicherheitsvorfall ziehen zu können.

---

94 «Social Engineering Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Aktionen zu bewegen. Ein Angreifer kann mittels Social Engineering beispielsweise versuchen, an Benutzernamen und Passwörter von Mitarbeitern eines Unternehmens zu gelangen, indem er sich am Telefon als Systemadministrator oder Sicherheitsverantwortlicher ausgibt. Durch Vorgeben akuter Computerprobleme und Vortäuschen von Betriebskenntnissen (z. B. Namen von Vorgesetzten, Arbeitsabläufe, usw.) wird das Opfer so lange verunsichert, bis es die gewünschten Informationen preis gibt.» (MELANI 2020a).

95 Malware ist ein Sammelbegriff für Programme, welche dazu entwickelt wurden, Benutzern Schaden zuzufügen. Es gibt zahlreiche Unterarten von Malware, z.B., Viren, Trojaner oder Spyware. Alle verlaufen anders und haben verschiedene Aufgaben, aber das gemeinsame Ziel den Benutzern zu schaden. (MELANI 2020b).

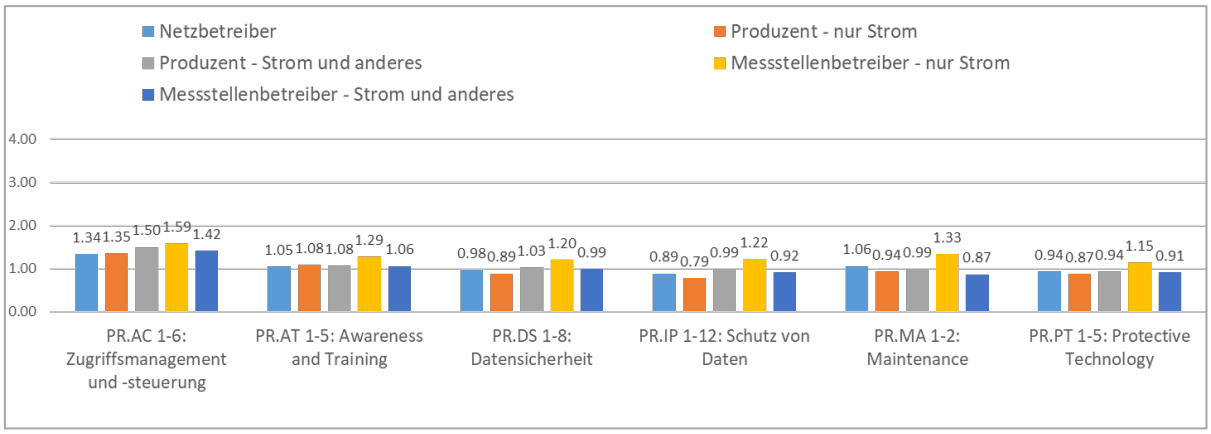


Abbildung 46: Maturität IT-Kategorie «Schützen»

In der **IT-Kategorie «Erkennen»** sind die Cyber-Fähigkeiten noch stark verbesserungswürdig. Das Erkennen von «Anomalien», sowie die «Security Operations» (SOC) Prozesse, welche der Unterkategorie «Vorfälle» zugehören, sind noch keineswegs befriedigend und befinden sich gar noch weit von der fundamentalen Maturitätsstufe 1 entfernt. Ein SOC ist eine Zentrale für alle sicherheitsrelevanten Services im IT-Umfeld von Unternehmen.[96] Das SOC integriert, überwacht und analysiert alles sicherheitsrelevanten Systeme wie Unternehmensnetzwerke, Server oder Internetservices. Unter anderem werden die Log-Dateien der einzelnen Systeme gesammelt, analysiert und nach Auffälligkeiten untersucht, Ebenso ist die Unterkategorie «Detection Process, für die Identifikation von Auffälligkeiten und sicherheitsrelevanten Ereignissen, essentiell wichtig, um potenzielle Auswirkungen eines Vorfalls zeitgerecht bekämpfen und vermindern zu können. Je eher Cyber-Sicherheitsvorfälle erkannt werden, desto besser für die Wirksamkeit der Reaktionsmassnahmen. Weiter ist das Schadenspotential einer früh gestoppten Attacke deutlich geringer da sich diese nicht noch länger innerhalb der Unternehmung verbreiten kann. Es besteht grundsätzlich die Annahme, dass solange die Stromproduktion oder –Lieferung nicht unterbrochen wird, die Cyber-Sicherheit grösstenteils gewährleistet ist. Dieses Paradigma verschiebt sich, wie bereits angesprochen, aber zunehmend zu der Anerkennung, dass alle drei Informationssicherheitsziele, die Verfügbarkeit, die Integrität und die Vertraulichkeit der Systeme, wesentliche Bestandteile für die Cyber-Sicherheit sind.

Branchenspezifische Computer Emergency Response Teams (CERTs) können bei der Cyber-Fähigkeit des «Erkennens» helfen indem einzelnen Unternehmen ihre Ressourcen bündeln, Erfahrungen teilen und mit immer professioneller werdenden Angreifern Schritt halten können. Die Kernaufgabe eines CERT ist die Prävention, Detektion und Bewältigung von IT- und Netzwerk-Vorfällen, welche seine Kunden betreffen. Das CERT-Team besteht aus IT-Sicherheitsspezialisten und arbeitet eng und auf hohem Vertrauensniveau mit seinen Kunden zusammen. Aufgrund der internationalen Dimension benötigt ein CERT-Team neben einem sehr guten nationalen auch ein weltweites Netzwerk von Vertrauensbeziehungen auf operativer IT-Security-Ebene. Im Gegensatz zu SOCs, sind CERTs eher eine Notfallorganisation, welche sich um detaillierte Analysen und sich mit der Behebung von Sicherheitsvorfällen beschäftigt. SOC und CERT ergänzen sich und bilden somit eine leistungsfähige Einheit für die Cyber-Sicherheit. Die Zusammenarbeit der Unternehmungen mit dem nationalen CERT (GovCERT), welches in dem nachfolgenden Kapitel zu dem regulatorischen Umfeld genauer erläutert wird, ist essentiell um einen kontinuierlichen Wissensaustusch bezüglich der Threat Intelligence sicherzustellen. Threat Intelligence ist eine relativ junge Disziplin und ein solcher Service liefert aktuelle Informationen zur Cyber-Bedrohungslage damit Unternehmen einen Wissensvorsprung bezüglich wie und was für ein Angriff erfolgen könnte und sich entsprechend dagegen wappnen kann. Daraus ergeben sich unter Anderem konkrete Handlungsempfehlungen und Hilfestellungen für Marktteilnehmer.[97] Zudem können branchenspezifische CERTs helfen, Stromsektor-spezifische Cyber-Gefahren zu erkennen. Beispielsweise fördert die im Juni 2019 gestartete Initiative von Swisspower zusammen mit der Stiftung SWITCH die Kooperation für Cyber-Sicherheit in Stadtwerken mithilfe eines firmenübergreifenden Energie-CERT (Swisspower 2019). Zusammen mit SWITCH entwickeln die beteiligten Stadtwerke Abwehrstrategien

---

96 Luber & Schmitz (2017), Definition SOC.

97 European Union Agency for Cybersecurity (2018), Report - Exploring the opportunities and limitations of current Threat Intelligence Platforms.

gegen Cyberattacken und informieren sich gegenseitig über Bedrohungen.[98] Das Energie-CERT arbeitet zudem mit dem Cyber-Defence-Campus der Armasuisse zusammen. Diese Kooperation wurde ausdrücklich vom BFE begrüsst.

Das momentan fehlende Monitoring über allfällige Vorfälle ist jedoch bedenklich vor allem in Bezug auf die angenommenen Cyber-Risiken «Verlust der Integrität der Daten» und «Advanced Persistent Threat (APT)»[99], welche von Netzbetreibern als zwei der sechs Hauptrisiken in der ElCom Studie identifiziert wurden.[100] Beide Risiken werden aufgrund deren Raffinesse meist nur durch kontinuierliches Testen der Prozesse und der Überprüfung der Aufzeichnung und Dokumentation (Logging) entdeckt. Vor allem APTs sind sehr schwer erkennbar und zeigen, dass auch schwere Cyber-Sicherheitsvorfälle beim Risikomanagement nicht ausser Acht gelassen werden dürfen.

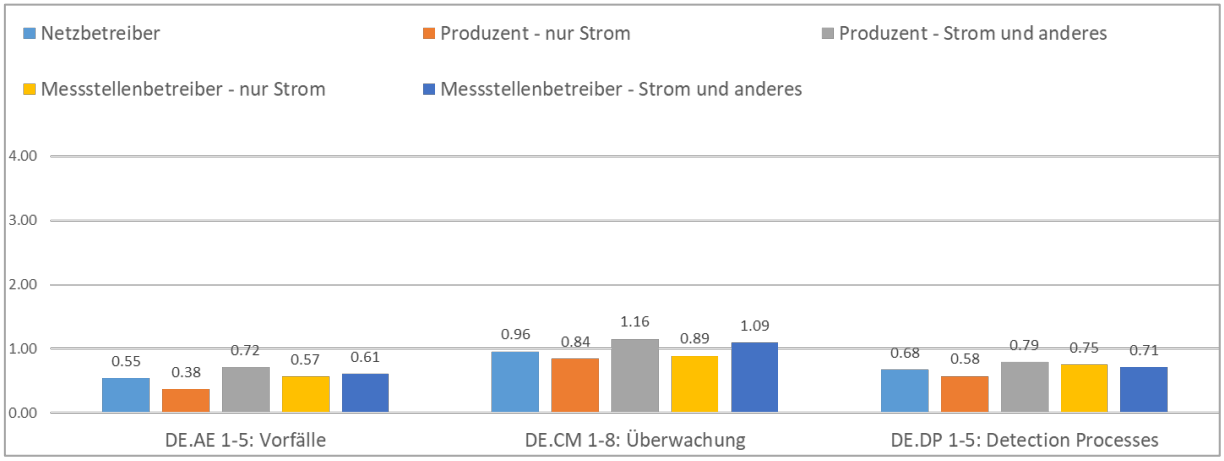


Abbildung 47: Maturität IT-Kategorie «Erkennen»

98 Vier schweizerische Stadtwerke sind bereits Teil dieser Plattform und sukzessive soll diese Teilnahmebasis erweitert werden. Die Namen die teilnehmenden Stadtwerke ist nicht veröffentlicht und es ist unklar ob die Teilnehmer der BFE-Umfrage an dieser Initiative beteiligt sind.

99 Ein APT ist Netzwerk-Angriff, bei dem sich eine unautorisierte Person Zugriff auf ein Netzwerk verschafft und sich dort so lange wie möglich unentdeckt aufhält. Die Intention eines APT-Angriffs ist in erster Linie, Daten zu stehlen und keinen sonstigen Schaden anzurichten. Ziel solcher APT-Angriffe sind oftmals Organisationen in Bereichen, bei denen sehr wertvolle Informationen zu holen sind. Das Informationssicherheitsziel der Integrität schützt primär vor solchen Attacken. (MELANI 2020b).

100 Eidgenössische Elektrizitätskommission (2019), Bericht - Cyber-Sicherheit 2019.

Innerhalb der **IT-Kategorie «Reagieren»** auf IT-Sicherheitsvorfälle liegen teils weit unter der Maturitätsstufe 1, die vorhanden Fähigkeiten scheinen daher allgemein bescheiden zu sein. Die Werte betreffend «Response Planning» unterstreichen lassen erahnen, dass die meisten Vorfälle ad-hoc operativ abgehandelt werden ohne bereits vordefinierten Prozessabläufen zu folgen. Dieses Bild der ad-hoc Anpassung der Sicherheitsmassnahmen wird ebenfalls in dem Bericht der ElCom für die Unternehmenskategorie der Netzbetreiber bestätigt.[101] Es fehlt demnach an Reaktionsplänen im Ereignisfall und die Cyber-Risiken werden kaum vollumfänglich adressiert. Vordefinierte Prozesse, Strategien und Verantwortlichkeitsbereiche würden helfen, die weitere Ausbreitung eines Cyber-Sicherheitsvorfalls zu verhindern und den möglichen Schaden zu begrenzen.

Auch die fehlenden Kompetenzen im Bereich der «Analyse» verhindern eine adäquate Reaktion, da einerseits relevante Benachrichtigungen aus Detektionssystemen nicht die benötigten Nachforschungen auslösen und anderseits die Auswirkungen eines Cyber-Sicherheitsvorfalls nicht korrekt erkannt werden können. Neben SOC-Playbooks[102] würden hier gewisse IT-Tools wie beispielsweise Security Information and Event Management (SIEM)[103] - und Security Orchestration and Automated Response (SOAR)[104] Lösungen helfen.

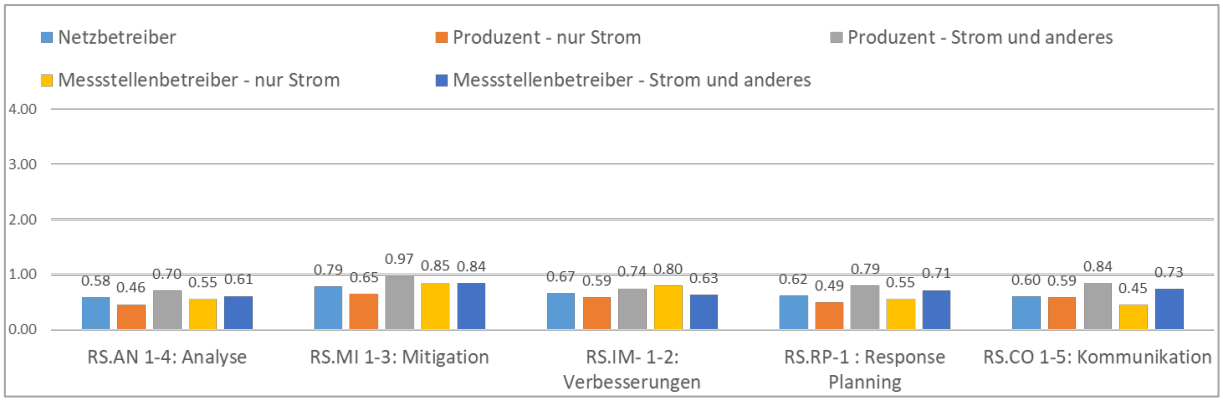


Abbildung 48: Maturität IT-Kategorie «Reagieren»

[101] Eidgenössische Elektrizitätskommission (2019), Bericht - Cyber-Sicherheit 2019.

[102] SOC-Playbooks bestehen aus vordefinierten Prozessen, welche je nach korrespondierendem Cyber-Sicherheit-Vorfall ausgelöst werden. Es hilft den SOC-Mitarbeitern die Bedrohungslage möglichst schnell einzudämmen und Gegenmassnahmen zu ergreifen. (Luber & Schmitz 2017).

[103] Das SIEM ermöglicht einen ganzheitlichen Blick auf die IT-Sicherheit, indem Meldungen und Logfiles verschiedener Systeme gesammelt und ausgewertet werden. Verdächtige Ereignisse oder gefährliche Trends lassen sich in Echtzeit erkennen. (Luber & Schmitz 2017).

[104] Ein SOAR stellt Software und Verfahren zur Verfügung, mit denen sich Informationen über Sicherheitsbedrohungen sammeln lassen. Auf deren Basis erfolgt eine automatische Reaktion. Ziel ist es, das Bedrohungs- und Schwachstellenmanagement in einem Unternehmen zu verbessern. (Luber & Schmitz 2020).

In Anbetracht der **IT-Kategorie «Erholen»** von IT-Sicherheitsvorfällen scheinen rudimentäre Recovery Strategien und Pläne gegeben zu sein, denn immerhin werden bei der Unterkategorie «Wiederherstellungspläne» Werte um die Maturitätsstufe 1 erreicht. Das Definieren der benötigten Kommunikationswege und -abläufe mit internen und externen Parteien, Cyber-Fähigkeit «Kommunikation», scheint noch grösseres Verbesserungspotential aufzuweisen mit Werten deutlich unter Maturitätsstufe 1. Die Wiederherstellungsplanung muss sichergestellt sein, damit eine zeitnahe Erholung eines allfälligen Cyber-Sicherheitsvorfalls gewährleistet werden kann und das Unternehmen schnellstmöglich zu einem «Modus Operandi» zurückfinden kann. Die Unterkategorie der Kommunikation, welche primär die Koordination für die Wiederherstellungsaktivitäten mit internen und externen Partnern (z.B., Behörden oder CERTs) betrifft, ist unter anderem bedeutend damit die öffentliche Wahrnehmung aktiv angegangen werden kann und die eigene Organisation nach einem eingetretenen Cyber-Sicherheitsvorfall wieder positiv wahrgenommen werden kann. Eine regelmässige, proaktive Kommunikation mit den relevanten Stakeholdern bereits vor einem Vorfall ist zu bevorzugen, da die eigene Position so zumeist sachlicher dargestellt werden kann und eine gewisse Vertrauensbasis vorhanden ist.

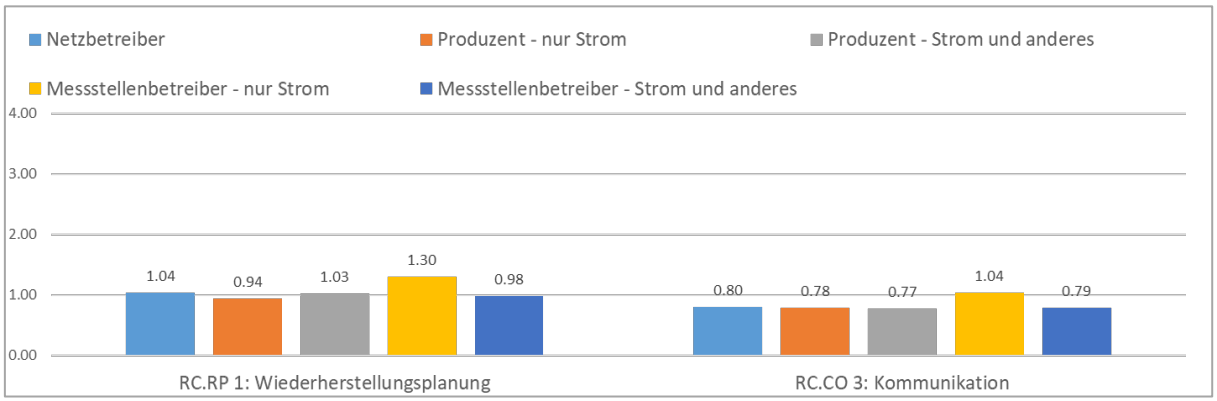


Abbildung 49: Maturität IT-Kategorie «Erholen»

1.2.2 Auswertung Modul 3: aktuelles OT-Maturitätsniveau

In Kapitel 3 wurde eine Gesamtübersicht über die fünf IKT Minimalstandard Funktionen dargelegt (vgl. Abbildung 10). In diesem Kapitel werden die einzelnen Kategorien genauer analysiert und entlang den 23 Cyber-Fähigkeiten bezüglich der OT-Sicherheit ausgewertet.

Innerhalb der **OT-Kategorie «Identifizieren»** zeigt sich, dass den Unternehmen die Risiken in der OT-Landschaft tendenziell unbekannt sind. Bis anhin wurde offenbar in der Regel versucht, als Sicherheitsstrategie OT-Netzwerke und Systeme stets komplett physisch von der IT-Landschaft abzugrenzen. Die Identifikation von Sicherheits-Risiken beschränkte sich daher primär auf physische Sicherheitsparameter (z.B., 24/7 Überwachung der Anlagen, physischer Zugang) und der Fokus lag auf der ständigen Verfügbarkeit der Systeme.

Jedoch zeigen jüngste technologische Trends eine Tendenz in Richtung grösserer Vernetzung und der Schaffung neu vorhandener Schnittstellen zwischen der OT, sowie vorhandenen IT-Landschaft. Beide Entwicklungen schaffen neue Gefahren und grössere Angriffsflächen für die OT-Umgebung aus einer Cyber-Perspektive.

Durch die daraus resultierenden neuen Gefahren und Cyber-Angriffsmöglichkeiten befindet sich die Cyber-Risikolandkarte der Unternehmen für OT-Sicherheit derzeit in einem starken Wandel. Viele der Betriebe sind sich diesen neuartigen Cyber-Risiken nicht bewusst. Das Risikomanagement verbunden mit einem ISMS, welches auch die OT-Landschaft mitabdeckt, wäre ein wichtiges Hilfsmittel, um dieses veränderte Geschäftsumfeld den Elektrizitätsunternehmen zu verdeutlichen und zu konkreten Aktionen anzuregen. Offenbar scheint dies aber nur im rudimentären Ansatz implementiert zu sein, die Maturitätsstufe beim «Risikomanagement» sind tief (Werte zwischen 0.56 und 0.87) und zeigen auf, dass keine entsprechenden Prozesse formalisiert sind. Das «Inventar Management» für OT-bezogene Assets (OT Systeme, Messgeräte, Sensoren, OT-Netzwerkbezogene Komponenten, etc.) wird meist dezentral direkt in den jeweiligen Werken individuell verwaltet. Aus diesem Grund sind tieferen Werte, zwischen 0.79 und 1.08, verglichen mit der IT-Seite, Werte zwischen 1.03 und 1.25, nachvollziehbar, da eine zentrale Sicht und Standardisierung meist fehlt. Dies wird auch durch die Electrosuisse Umfrage unterstützt, welche nur bei wenigen mittleren Werken, die Inventarisierung, Klassierung und Risikobewertung von Hardware, Software und Daten, als zufriedenstellend taxiert.[105] Ohne diese Angaben fehlen grundlegende Informationen, welche zentral für die Definition der Ziele und die Zuweisung von der Verantwortlichkeit innerhalb des Unternehmens sind.

[105] Electrosuisse (2019), Cybersecurity bei kleinen und mittleren Elektrizitätsversorgungsunternehmen.

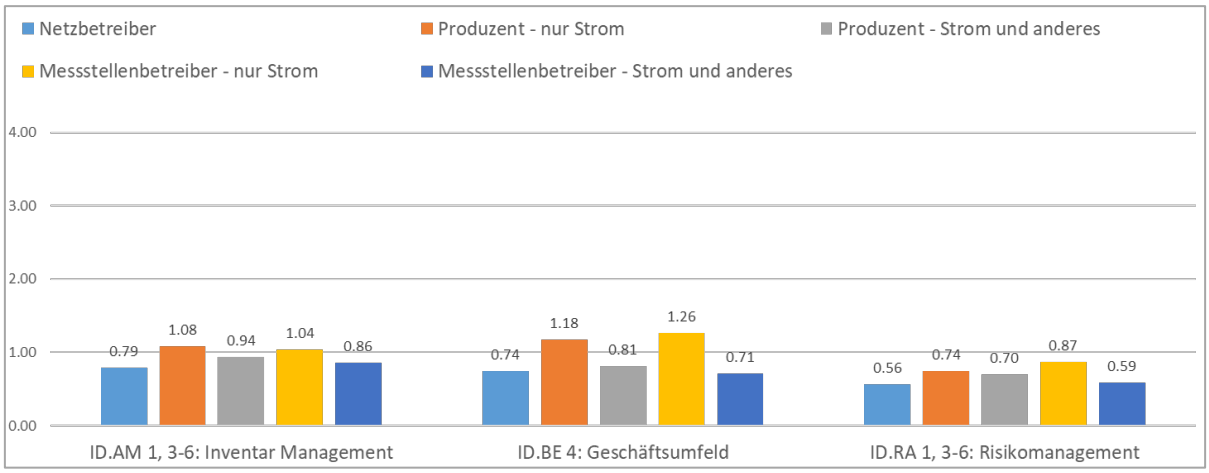


Abbildung 50: Maturität OT-Kategorie «Identifizieren»

In der **OT-Kategorie «Schützen»** stechen insbesondere der Schutz von Daten, sowie das Zugriffsmanagement positiv im Vergleich zu andere Kategorien hervor. Die Maturitätsniveaus befinden sich klar über der 1 und der Höchstwert von 1.6 bei der Fähigkeit «Schutz von Daten» wird gar erreicht. Dieses Bild ist wohl so zu begründen, dass OT-Landschaften in der Energie in der Regel in einer von der IT abgeschotteten, eigenen Infrastruktur betrieben werden und es sich bei den Systemen (SCADAs, etc.) meist um bereits gehärtete Standardlösungen von Drittanbietern handelt. Bei dem Zugriffsmanagement ist hinzuzufügen, dass in vielen Industrielle Steuerungssystemen (ICS), welche der OT zuzuordnen sind, verschiedene Systeme von einer Vielzahl unterschiedlicher Benutzer verwendet werden. Diese Systeme müssen oft schnell zugänglich sein, wie es z.B. der Systembetrieb erfordert, und sind zudem herausfordernd für unternehmenssichere Authentifizierungs-, Berechtigungs- und Kontoverwaltungsmethoden, da ICSs 'immer eingeschaltet' sind. Diese Gegebenheiten stehen vielfach in Gegensatz zu den Anforderungen der OT-Sicherheit denn mit einer zunehmenden Vernetzung steigt auch die Gefahr einer rasanten Verbreitung von Schadsoftware. Rollenbasierte Berechtigungskonzepte[106] und «Zero-Trust»-Modelle[107] sind daher essentiell für eine nachhaltige Zugangskontrolle. Dies kann zentral in einem ISMS gesteuert werden und das Zugriffsmanagement weiter stärken.

Die vergleichsweise tiefe Maturität, mit den meisten Werten unter der Basisstufe 1, im «Awareness & Training»-Bereich ist darauf zurückzuführen, dass sich OT-Eigentümer und Besitzer auf ihr System- und Prozesswissen verlassen um das ordnungsgemässe Funktionieren, und somit primär die Verfügbarkeit, der Systeme zu gewährleisten. Jedoch mit der steigenden Vernetzung und der Zunahme von Cyber-Bedrohungen ist es für Unternehmen entscheidend, dass sie ihre Mitarbeiter sensibilisieren und auch schulen um die oft ausgenutzte «Schwachstelle Mensch» zu verringern.

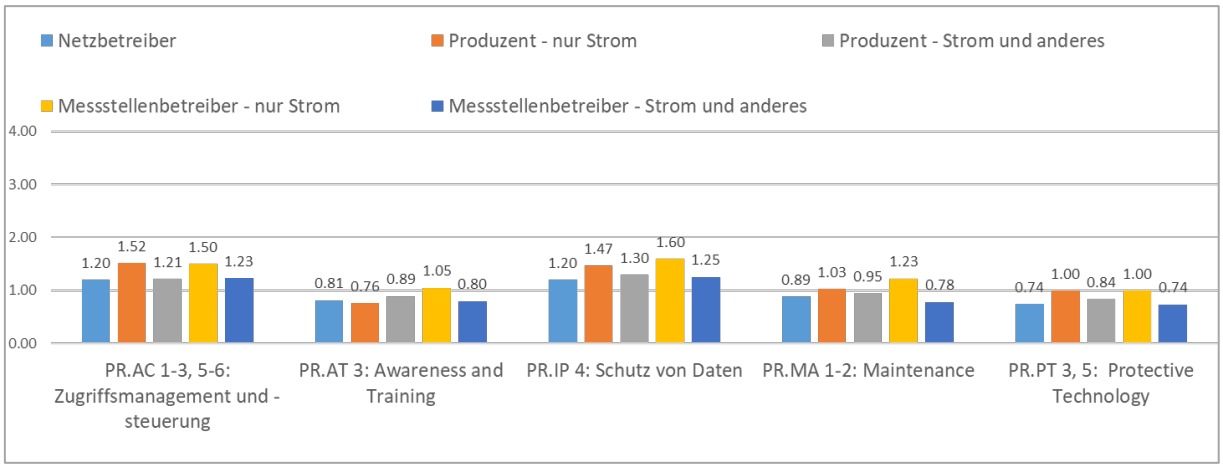


Abbildung 51: Maturität OT-Kategorie «Schützen»

[106] Rollenbasierte Berechtigungskonzepte ist ein Netzwerksicherheitsparadigma, bei dem den Benutzern im Netzwerk Berechtigungen basierend auf ihrer Rolle im Unternehmen gewährt werden. (MELANI 2020a).

[107] Zero Trust-Sicherheit verlangt, das alte Paradigma „vertraue, aber kontrolliere" aufzugeben und zu einem neuen Paradigma „vertraue nie, kontrolliere immer" bei den Zugriffsberechtigungen überzugehen. (IKT Minimalstandard).

Wie zu erwarten sind die Fähigkeiten in der **OT-Kategorie «Erkennen»** insgesamt tief. Die benötigten, technischen Fähigkeiten um Sicherheits-Monitoring der OT-Landschaft zentral erfolgreich zu betreiben etablieren sich generell erst seit kurzem am Markt und es handelt sich daher um eine relativ «junge» Sicherheitsdisziplin. Interessanterweise weist aber die OT-Subkategorie «Vorfälle» bei allen Unternehmenstypen eine höhere Maturität (Werte zwischen 0.72 und 0.89) auf als die korrespondierende IT-Unterkategorie (Werte zwischen 0.38 und 0.72). Netzbetreiber und Produzenten haben oftmals Notfallteams, welche 24/7 vor Ort sind, um die operative Überwachung verschiedener Anlageparameter (z.B. Spannung, Stromstärke, Druck) zu messen. So werden Unregelmässigkeiten frühzeitig entdeckt und es kann bei Bedarf direkt eingriffen werden. Die entsprechenden Kompetenzen im IT-Sicherheitsbereich im Sinne eines lokalen SOCs und dem Monitoring des SIEMs sind hier weniger ausgreift.

Die Subkategorie «Detection Processes» ist ähnlich tief bei der OT- und IT-Landschaft (IT-Sicherheit Werte zwischen 0.58 und 0.79; OT-Sicherheit Werte zwischen 0.5 und 0.78). Der Einsatz von Überwachungs-Systemen, welche anomale Verhaltensweisen und Angriffssignale erkennen bringen zusätzliche Komplexität in eine OT-Umgebung, aber unerlässlich um mögliche Sicherheitsvorfälle frühzeitig erfassen und bekämpfen zu können. Entscheidende Mechanismen sind hierbei die Durchführung gründlicher, unabhängiger und regelmässige Audits des Sicherheitsstatus, sowie die Überwachung der Informationsrisiken damit die rechtlichen, regulatorischen und vertraglichen Anforderungen sichergestellt werden können.

Des Weiteren, ist die Erkenntnis, dass ein Cyber-Angriff trotz starken Abwehrmassnahmen nicht garantiert verhindert werden kann, essentiell um diese kritische Funktion stärken zu können. Die Erweiterung der Informationssicherheitsziele von einem singulären Fokus auf die Verfügbarkeit hinzu zu der Einbeziehung von Integrität und Vertrautheit ermöglicht eine weitreichendere Übersicht über den gesamten OT-Bereich, welcher geschützt werden muss. Der OT-Bereich kann nicht mehr abgeschottet werden und daher gewinnt die Erkennung von Cyber-Sicherheitsvorfällen immer mehr an Bedeutung.

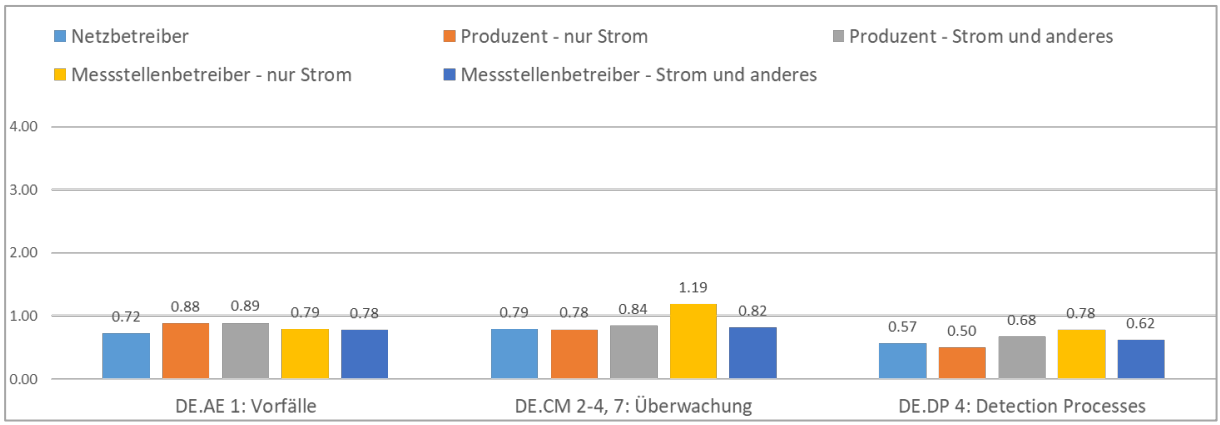


Abbildung 52: Maturität OT-Kategorie «Erkennen»

In der **OT-Kategorie «Reagieren»** zeigt sich ein ähnliches Bild wie bei der OT-Kategorie «Erkennen» und lässt sich ebenfalls als unbefriedigend bzw. die Maturität als sehr tief bezeichnen. Die Maturitätsstufen befinden sich teils sehr stark unter dem Niveau 1. Bemerkenswert sind hier die Messstellenbetreiber, die offenbar etwas besser organisiert sind als die anderen Unternehmen. Sie sind in allen Unterkategorien am besten aufgestellt. OT-Systeme sind oftmals geschlossene Systeme von Drittanbietern, welche daher auch nur bedingt eine Reaktion durch die Umfrage-Teilnehmer selbst ermöglichen. Meist müssen die Hersteller direkt in die Pflicht genommen werden. Die Unternehmungen müssen somit sicherstellen, dass ihre Hersteller Benachrichtigungen aus Detektionssystemen berücksichtigt, dies Nachforschungen auslöst und so schnell wie möglich auch den Kunden mitteilt. Meist sind diese Detektionssysteme im Rahmen des operativen Monitorings nur auf die Verfügbarkeit der Anlagen ausgerichtet, um konkrete Ausfälle zu erkennen. Vorgängige verdächtige Aktivitäten werden nur selten erkannt. Ein SOC hilft in diesem Rahmen des Sicherheits-Monitoring, Unregelmässigkeiten in den Systemen des Herstellers zu erkennen und die Reaktion frühzeitig zu initiieren.

Trotz dieser teils externen Abhängigkeit, ist es kritisch, dass Unternehmen einen Reaktionsplan zur Adressierung bekannter Cyber-Sicherheitsvorfälle erarbeitet haben um diesen im Ereignisfall korrekt und zeitgerecht ausführen zu können. Der Cyber-Fähigkeit der «Kommunikation» wird hierbei typischerweise zu wenig Aufmerksam geschenkt mit Werten, welche sich gerade zwischen den Maturitätsstufen 0 und 1 befinden, ist jedoch wichtig damit alle Personen ihre Aufgaben und die Reihenfolge ihrer Handlungen kennen bezüglich der Reaktion auf eingetretener Ereignisse. Übungen zu Cyberkrisen ermöglichen es Mitarbeiter auf diese Prozesse zu sensibilisieren und die Handlungsweisen weit möglichst zu automatisieren.

Die Unternehmen selbst können weiter gezielt durch die Etablierung eines eigenen CERTs oder durch die Teilnahme einen branchenspezifischen CERTs ihre Cyber-Fähigkeiten in der Gesamtkategorie «Reagieren» stärken. Diese gewinnt zunehmend an Bedeutung, da erkannt wird, dass keine 100-prozentige Sicherheit möglich ist. Die schnelle und effektive Abschwächung eines identifizierten Cyber-Sicherheitsvorfäll ist kritisch um den Schaden zu begrenzen.

Eine weitere relevante Massnahme in dieser Kategorie ist die Meldung von Cyber-Sicherheitsvorfälle an CERTs oder an andere relevante Instanzen gemäss den vorliegenden Regulierungen. Wie bereits angesprochen, gibt es momentan keine Meldepflicht von Cyber-Sicherheitsvorfällen für Betriebe im Schweizer Strommarkt.

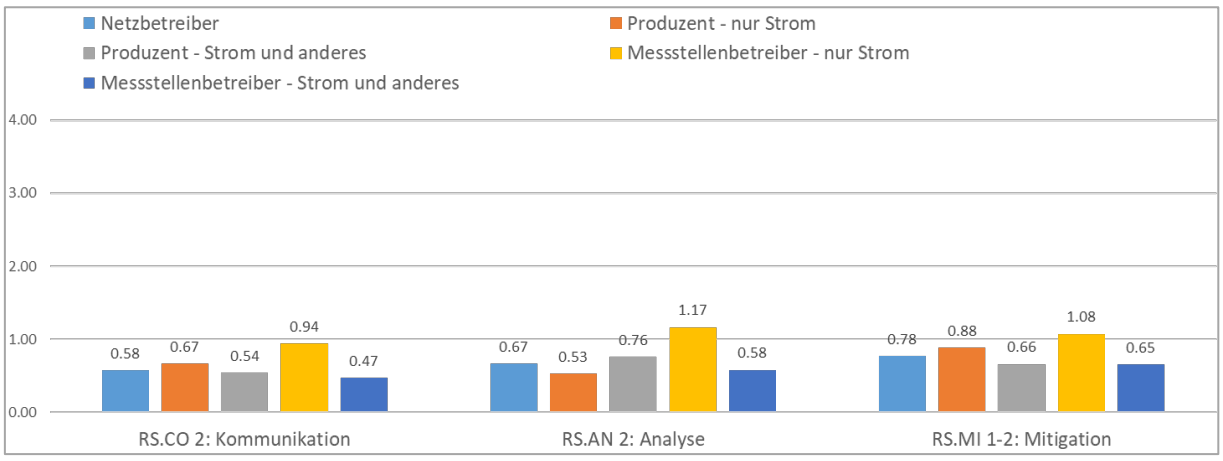


Abbildung 53: Maturität OT-Kategorie «Reagieren»

Die Resultate in der letzten **OT-Kategorie «Erholen»** nach Sicherheitsvorfällen sollten vor dem Hintergrund der Ergebnisse in den anderen Kategorien kritisch betrachtet werden, da die Rückkehr zu einem «Modus Operandi» nach einem Cyber-Vorfall anscheinend auf ad-hoc Massnahmen besteht und die Betriebe über keine vorausschauende Planung hierfür verfügen. Auch hier stechen die Messstellenbetreiber heraus, aufgrund der vergleichsweise starken Werten gerade über der Maturitätsstufe 1. Bei der «Wiederherstellungsplanung» in der OT-Sicherheit ist es empfehlenswert, die betroffenen Komponenten direkt zu isolieren und auszutauschen und/oder auf alternative, bereits vorhandene Systeme auszuweichen, damit eine hohe Verfügbarkeit trotz Cyber-Vorfall garantiert werden kann. Es ist anzunehmen, dass solche Strategien basierend auf den tiefen Werten bei den Unternehmen wenig bekannt sind.

Die Unterfunktion der «Verbesserung» ist typischerweise mit einer höheren unternehmerischen Maturität verbunden, da gewisse Grundstrukturen bereits bestehen müssen um diese weiter optimieren zu können. Da die Elektrizitätsunternehmen generell sehr tiefe Maturitätswerte haben, ist es daher nicht verwunderlich, dass diese Maturitätsstufe ebenfalls tief ist. Grundlage zur kontinuierlichen Verbesserung ist eine lückenlose Dokumentation sämtlicher Cyber- Sicherheitsvorfälle damit die notwenigen Lehren aus der Analyse gezogen werden können um dass die eigenen Prozesse dynamisch anpassen zu können. Die Gegebenheiten des OT-Bereichs können jedoch die Ermittlung zu der Ursache eines Cyber-Vorfalls hindern, da die betroffenen Systeme meist nicht ausser Betrieb genommen werden, um weiterhin verfügbar zu sein. Dadurch wird die Beweisaufnahme verhindert und die Verbesserungsmöglichkeiten aufgrund von fehlenden Evidenzen beeinträchtigt. Dies unterstreicht, weshalb die oben genenannten Strategien so wichtig wären innerhalb der «Erholen»-Kategorie.

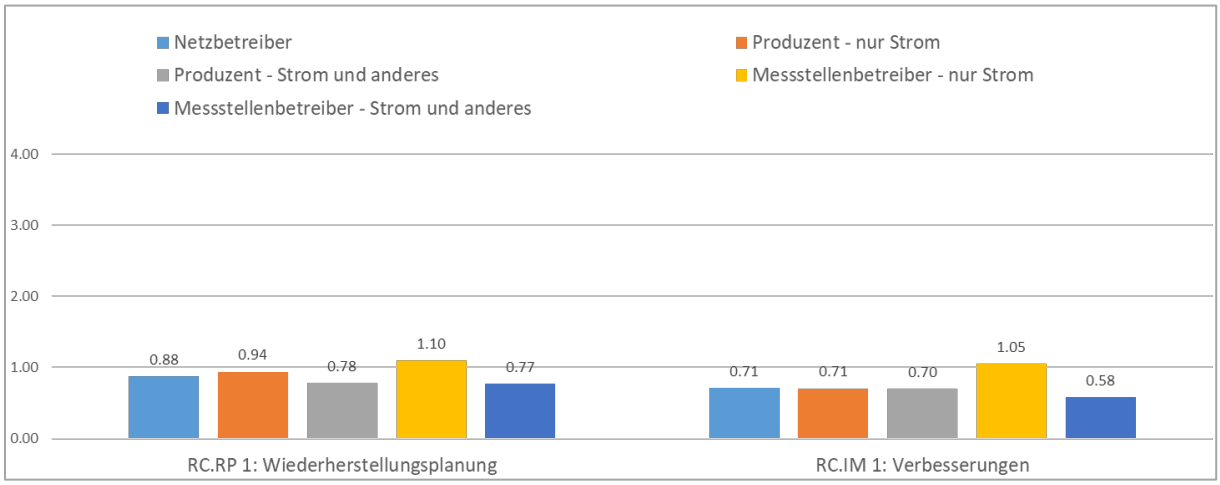


Abbildung 54: Maturität OT-Kategorie «Erholen»

1.4 Analyse Modul 4: Weitere Erkenntnisse und Auffälligkeiten

Modul 4 wurde entlang verschiedener Themenbereiche ausgewertet, um tiefere, weiterführende Erkenntnisse und Auffälligkeiten gewinnen zu können. Diese Beantwortung hierauf ist essentiell um die aktuelle Situation der Unternehmen der Elektrizitätswirtschaft bezüglich IT-/OT-Maturität besser korrelieren zu können und mögliche Schlussfolgerungen zu ihren Schwächen und Stärken in den verschiedenen Bereichen verstehen zu können.

Vorhandensein einer IT-/OT-Strategie

Netzbetreiber, Produzenten und Messstellenbetreiber scheinen generell in einer ähnlichen Lage zu sein und rund 50% der Teilnehmer verfügen über eine explizite IT-/OT-Strategie. Es ist ein positiver Trend zu sehen, dass viele der übrigen Betriebe diesen Punkt in naher Zukunft ebenfalls noch adressieren wollen.

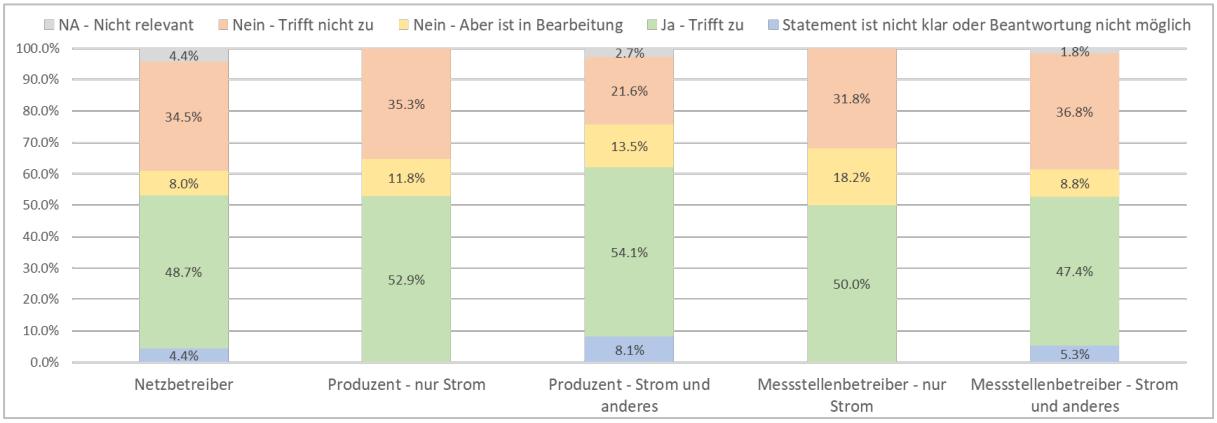


Abbildung 55: Vorhandensein einer Unternehmensweite IT-/OT-Strategie

Vergleicht man das Vorhandensein einer expliziten IT-Strategie mit den aktuellen Maturitätsgraden der IT-Sicherheit, so sticht ins Auge, dass eine starke, positive Korrelation zwischen dem Vorhandensein einer IT-Strategie, sowie dem aktuellen Maturitätsgrad im Bereich IT-Sicherheit besteht. Jene Unternehmen, welche über eine Strategie verfügen, erreichen Werte klar über der Maturitätsstufe 1. Selbst jene Unternehmen, welche angeben, dass diese Strategie in Bearbeitung sei, weisen eine deutlich höhere Maturität (zwischen Maturitätsstufe 0 und 1) auf als jene die die Frage verneinten (nah an Maturitätsstufe 0). Eine IT-Strategie ist folglich ein wichtiger Bestandteil, für die Weiterentwicklung der IT-Sicherheitsmaturität. Es ist eindeutig, dass eine Strategie es Unternehmen erlaubt Chancen und Risiken im IT-Bereich bewusster und strukturierter abzuwägen, ob sie diese Risiken eingehen oder vermindern wollen. Sie setzt zudem wichtige Prioritäten und Ziele explizit fest. Dieser geführte Prozess ermöglicht es den Betrieben genau zu verstehen, wo ihre Bedürfnisse in dem IT-Bereich liegen.

Es kann weiter angenommen werden, dass die «Statement nicht klar oder die Beantwortung nicht möglich sei»-Gruppe, auch über keine IT-Strategie verfügt und daher in die Nein-Kategorie fliessen würde. Dies beeinflusst die Beobachtung bezüglich der relativen Verteilung zwischen den Korrelationsgruppen kaum.

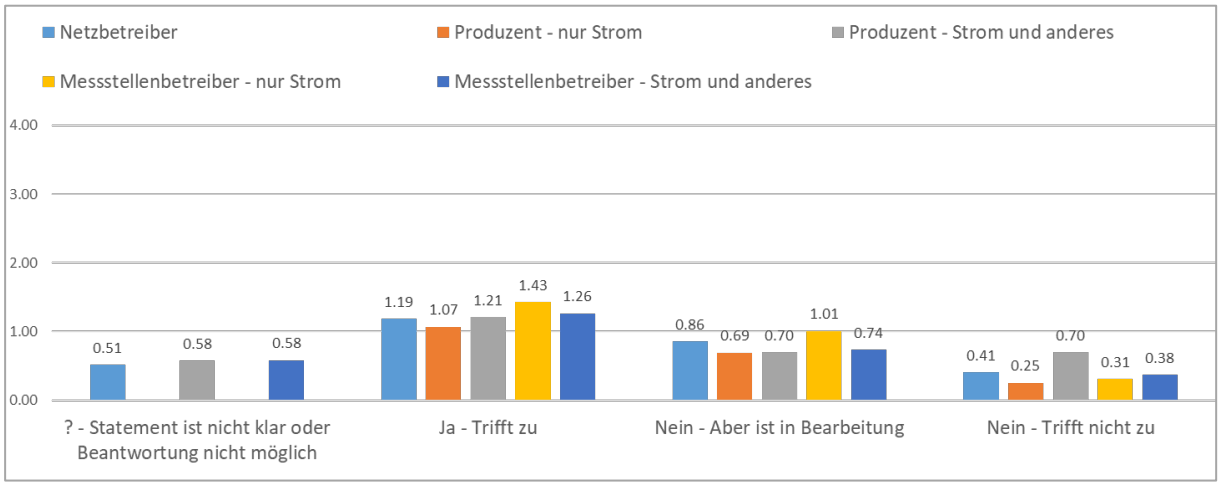


Abbildung 56: Durchschnittlicher IT-Maturitätsgrad in Korrelation mit dem Vorhandensein einer Strategie für IT-Sicherheit

Korreliert man das Vorhandensein einer expliziten OT-Strategie mit den aktuellen Maturitätsgraden der OT-Sicherheit, so wiederholt sich dasselbe Bild einer stark positiven Korrelation zwischen den beiden Faktoren. Die Werte der Messstellenbetreiber für nur Strom sind für die IT- sowie OT-Sicherheit in Korrelation mit dem Bestand der jeweiligen Strategie beachtenswert im positiven Sinne. Aus Abbildung 36 ergibt sich, dass gewisse Unternehmen gar zu Maturitätsniveau 2 «partiell umgesetzt, vollständig definiert und abgenommen» tendieren. OT-Sicherheit wird somit für jene Betriebe als permanenter Prozess und nicht als Zustand verstanden. Dies bedeutet, dass die Sicherheit kontinuierlich adressiert wird, da eine einmalige Berücksichtigung als Bestandsaufnahme nicht reicht, um langfristig Risiken bekämpfen zu können. Die Ansicht, Sicherheit als fortwährender Prozess zu betrachten, vermindert ad-hoc Anpassungen an Sicherheitsaspekte und stellt sicher, dass Cyber-Risiken werden besser und nachhaltiger gemanagt werden.

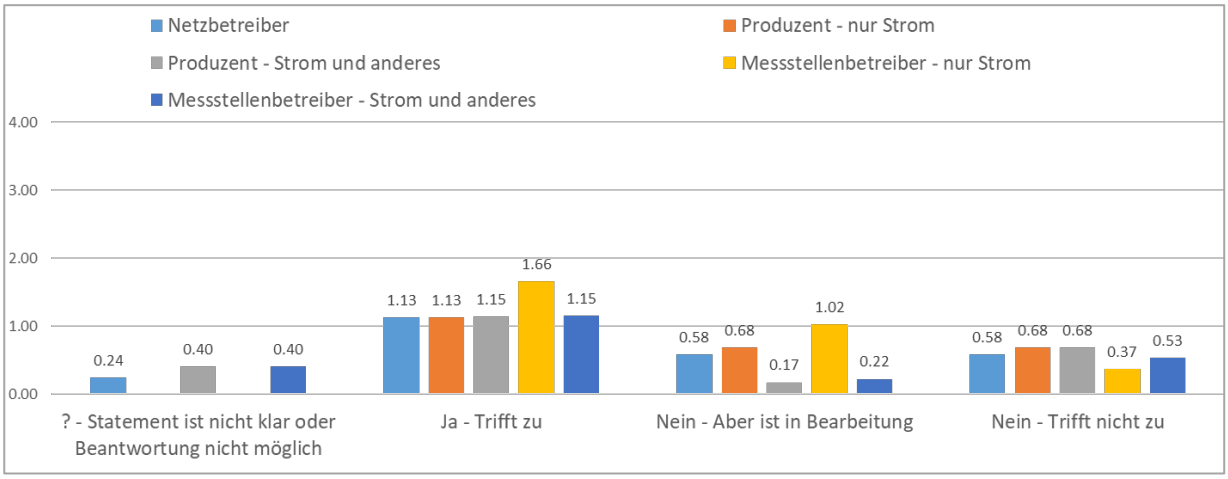


Abbildung 57: Durchschnittlicher OT-Maturitätsgrad in Korrelation mit dem Vorhandensein einer Strategie für OT-Sicherheit

Priorisierung IT- vs. OT-Sicherheit

Rund 62% aller Umfrageteilnehmer gaben an, dass sie die Sicherheit im IT- und OT-Bereich in etwa als gleich wichtig einstufen (Kategorie «Ja»). 20% der Befragten gaben an IT-Sicherheit mehr zu gewichten (Kategorie «Nein, IT-Sicherheit liegt im Vordergrund») versus 15% berücksichtigen die OT-Sicherheit stärker (Kategorie, «Nein, OT-Sicherheit liegt im Vordergrund»). Abbildung 37 stellt dar, welche Unternehmenstypen jeweils die OT- und/oder IT-Sicherheit priorisieren. Die Prozente über den Blöcken zeigt jeweils auf, wie viele des entsprechenden Unternehmenstyps entlang derselben Kategorie geantwortet haben.

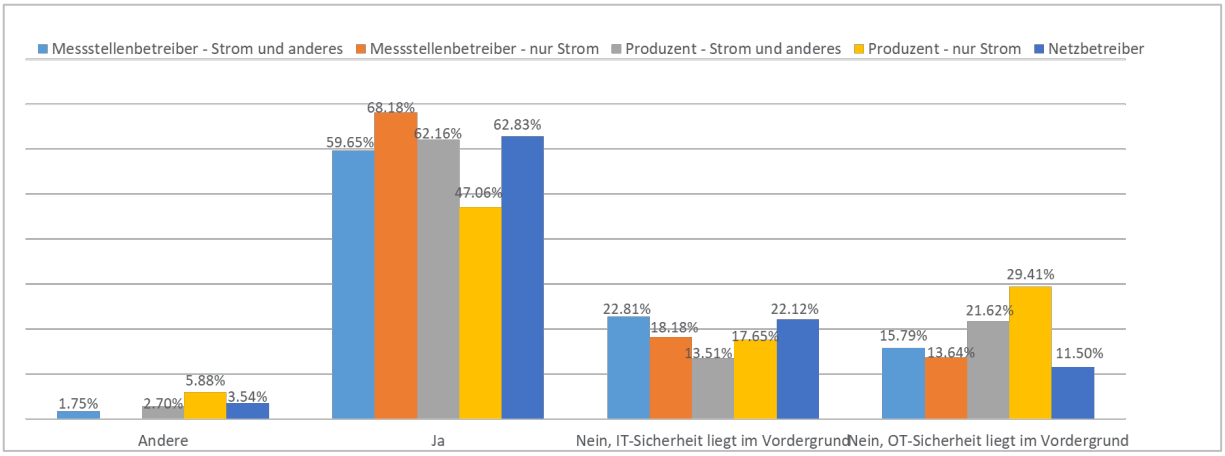


Abbildung 58: Priorisierung der IT- und/oder OT-Sicherheit

Eine interessante Korrelation ergibt sich aus Abbildung 58, welche zeigt, dass die niedrigsten Durchschnitts-Maturitätswerte von den Umfrageteilnehmern erzielt wurden, welche nach eigenen Angaben die IT-Sicherheit aktuell stärker gewichten (Durchschn. Maturität IT-Sicherheit = 0.42; Durchschn. Maturität OT-Sicherheit = 0.58). Die höchsten Werte erzielen Unternehmen, welche die OT-Sicherheit priorisieren (Durchschn. Maturität IT-Sicherheit = 0.99; Durchschn. Maturität OT-Sicherheit = 1.03). Die Kolorierung verdeutlicht die Maturitätsstufen indem tiefe Werte rot und hohe Werte grün gekennzeichnet sind. Die grundsätzliche Beobachtung bestärkt die Annahme, dass grundsätzlich jene Unternehmen, welche verstehen, dass die OT-Sicherheit immer vernetzter wird und nicht mehr physisch isoliert ist, die Cyber-Risiken auch dementsprechend besser managen.

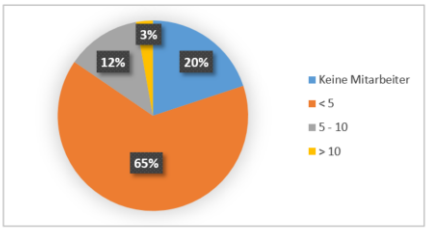
IT und OT Sicherheit gleich gewichtet?	Netzbetreiber	Produzent - nur Strom	Produzent - Strom und anderes	Messstellenbetreiber - nur Strom	Messstellenbetreiber - Strom und anderes	Grand Total
Andere						
Durchschn. Maturität - IT Sicherheit	0.55	1.23	1.30		1.30	**0.86**
Durchschn. Maturität - OT Sicherheit	0.21	0.87	0.40		0.40	**0.36**
Ja						
Durchschn. Maturität - IT Sicherheit	0.90	1.15	1.00	1.12	0.93	**0.96**
Durchschn. Maturität - OT Sicherheit	0.85	1.28	0.87	1.31	0.83	**0.92**
Nein, IT-Sicherheit liegt im Vordergrund						
Durchschn. Maturität - IT Sicherheit	0.49	0.21	0.25	0.53	0.35	**0.42**
Durchschn. Maturität - OT Sicherheit	0.68	0.76	0.14	0.74	0.48	**0.58**
Nein, OT-Sicherheit liegt im Vordergrund						
Durchschn. Maturität - IT Sicherheit	1.04	0.31	1.19	0.98	1.10	**0.99**
Durchschn. Maturität - OT Sicherheit	1.10	0.43	1.18	1.12	1.10	**1.03**

Abbildung 59: Korrelation zwischen der IT-/OT-Maturität und der Priorisierung der IT- und/oder OT-Sicherheit

Anzahl dezidierte IT-/OT-Sicherheitsmitarbeiter

Es lassen sich keine eindeutigen Korrelationen betreffend angegebenem Maturitätsniveau und Anzahl dedizierte Mitarbeiter für IT-/OT-Sicherheit erkennen. Dies dürfte primär daher der Fall sein, da die Angaben betreffend aktuelle Maturität auf einer Selbsteinschätzung beruhen anstelle einer objektiven Beurteilung durch Dritte oder mit konkreten Nachweisen. Diese Auffälligkeit in der Auswertung ist deshalb zu relativieren und es kann angenommen werden, dass tendenziell jene Unternehmen mit dezidierten IT-/OT-Mitarbeitern ein besseres Verständnis ihrer IT-/OT-Sicherheit haben und daher wahrscheinlich effektiv eine eher höhere Maturität aufweisen.

Anzahl Mitarbeiter IT / OT	Anzahl der Befragten
Keine Mitarbeiter	19,9%
< 5	64,6%
5 - 10	12,6%
> 10	2,8%
Insgesamt	**100,0%**



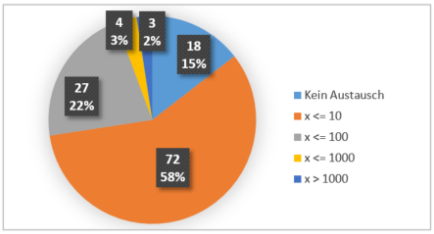
	Keine Mitarbeiter	< 5	5 - 10	> 10	Durchschnitt
Messstellenbetreiber - nur Strom					
Durchschnitt (IT)	1,98	2,02	2,36	1,00	1,99
Durchschnitt (OT)	2,53	1,88	2,67	1,89	2,17
Messstellenbetreiber - Strom und anderes					
Durchschnitt (IT)	1,67	1,80	2,28	1,51	1,83
Durchschnitt (OT)	1,58	1,76	2,37	1,06	1,79
Netzbetreiber					
Durchschnitt (IT)	1,70	1,82	2,25	1,32	1,81
Durchschnitt (OT)	1,86	1,74	2,30	1,46	1,82
Produzent - nur Strom					
Durchschnitt (IT)	1,37	1,86	1,92	1,00	1,74
Durchschnitt (OT)	1,88	1,85	2,11	1,89	1,92
Produzent - Strom und anderes					
Durchschnitt (IT)	1,76	1,88	2,28		1,95
Durchschnitt (OT)	1,23	1,73	2,37		1,82
Total Durchschnitt (IT)	**1,72**	**1,84**	**2,23**	**1,28**	**1,85**
Total Durchschnitt (OT)	**1,90**	**1,76**	**2,33**	**1,47**	**1,85**

Abbildung 60: Korrelation zwischen IT-/OT-Maturität und Anzahl dezidierter IT-/OT-Sicherheitsmitarbeiter

Automatisierter Datenaustausch mit Dritten

85% aller Befragten gaben an, dass sie Daten mit Externen automatisiert austauschen. Ein Grossteil der Teilnehmer (58%) betreibt einen automatisierten Austausch mit 10 oder weniger Teilnehmern. Es besteht jedoch keine eindeutige Korrelation zwischen der Cyber-Maturität und dem Austausch betreffend Daten mit Externen, wie die ähnliche Kolorierung in Abbildung 40 für den total Durchschnitt IT / OT verdeutlicht.

Anzahl der Parteien für Austausch	Anzahl der Befragten
Kein Austausch	18
x <= 10	72
x <= 100	27
x <= 1000	4
x > 1000	3
Grand Total	**124**



	Kein Austausch	x <= 10	x <= 100	x <= 1000	x > 1000	Durchschnitt
Messstellenbetreiber - nur Strom						
Durchschnitt (IT)		1,94	2,16	1,76		1,99
Durchschnitt (OT)		2,17	2,20	2,03		2,17
Messstellenbetreiber - Strom und anderes						
Durchschnitt (IT)	2,91	1,78	1,72	1,74	1,68	1,83
Durchschnitt (OT)	2,52	1,77	1,67	1,67	1,75	1,79
Netzbetreiber						
Durchschnitt (IT)	1,88	1,82	1,76	2,00	1,68	1,81
Durchschnitt (OT)	1,79	1,85	1,73	2,07	1,75	1,82
Produzent - nur Strom						
Durchschnitt (IT)		1,52	2,46			1,74
Durchschnitt (OT)		1,73	2,53			1,92
Produzent - Strom und anderes						
Durchschnitt (IT)	3,79	1,99	1,76	1,74	2,00	1,95
Durchschnitt (OT)	3,83	1,74	1,77	1,67	2,12	1,82
Total Durchschnitt (IT)	**2,23**	**1,82**	**1,82**	**1,86**	**1,76**	**1,85**
Total Durchschnitt (OT)	**2,10**	**1,84**	**1,81**	**1,89**	**1,84**	**1,85**

Abbildung 61: Korrelation Cyber Maturität mit automatisiertem Datenaustausch mit Externen

Auslagerung der IT- / OT-Umgebung an Dritte

Aus Abbildung 61 zeigt sich, dass fast 2/3 (61.79%) aller Umfrageteilnehmer angaben, dass sie bereits einen Teil Ihrer IT-Funktionen an Drittfirmen ausgelagert haben oder in absehbarer Zeit auslagern werden. Diese Entwicklung ist weitgehend unabhängig vom aktuellen Maturitätsgrad der Unternehmen betreffend IT-Sicherheit. Die grüne Kolorierung ist stärker, je höher der Maturitätswert. Dies soll visuell dazu beitragen, dass die durchschnittlichen Maturitätsniveaus leichter ersichtlich und so zu bewerten sind.

	Teil der IT-Funktionen sind bereits / werden in naher Zukunft an Drittfirmen ausgelagert	Durchn. Maturität - IT Sicherheit
Nein	**38.21%**	**0.88**
Netzbetreiber	16.67%	0.84
Produzent - nur Strom	2.85%	0.72
Produzent - Strom und anderes	5.69%	1.09
Messstellenbetreiber - nur Strom	2.44%	0.86
Messstellenbetreiber - Strom und anderes	10.57%	0.88
Ja	**61.79%**	**0.83**
Netzbetreiber	29.27%	0.80
Produzent - nur Strom	4.07%	0.75
Produzent - Strom und anderes	9.35%	0.86
Messstellenbetreiber - nur Strom	6.50%	1.04
Messstellenbetreiber - Strom und anderes	12.60%	0.79

Abbildung 62: Korrelation der Maturität mit IT-Auslagerung an Dritte

Im Vergleich hierzu haben rund 39% aller Umfrage-Teilnehmer angegeben, dass sie bereits einen Teil Ihrer OT-Funktionen an Drittfirmen ausgelagert haben oder in absehbarer Zeit auslagern werden. Hier zeigt sich eine tiefere OT-Maturität bei jenen Unternehmen, welche Teile der OT-Funktionen bereits auslagern oder dies in naher Zukunft tun werden (Durchschn. Maturität OT-Sicherheit = 0.67). Dies kann problematisch sein, vor allem in Anbetracht der generell tiefen Werte für das Lieferketten-Management (Werte zwischen 0.49 und 0.88). Es ist daher anzunehmen, dass die Unternehmen diese Verantwortung, welche durch die Auslagerung entsteht, momentan nicht wahrnehmen und die Risiken dementsprechend nicht gemangt werden. Die grüne Kolorierung zeigt auf den ersten Blick auf, dass diese Beobachtung insbesondere für Messstellenbetreiber nur Strom zutreffen zu scheint, da dieses Feld als einziges eine sättige Farbe aufzeigt.

	Teil der OT-Funktionen sind bereits / werden in naher Zukunft an Drittfirmen ausgelagert	Durchschn. Maturität - OT Sicherheit
Nein	**60.98%**	**0.96**
Netzbetreiber	26.83%	0.92
Produzent - nur Strom	4.07%	0.98
Produzent - Strom und anderes	10.98%	0.92
Messstellenbetreiber - nur Strom	4.07%	1.61
Messstellenbetreiber - Strom und anderes	15.04%	0.89
Ja	**39.02%**	**0.67**
Netzbetreiber	19.11%	0.67
Produzent - nur Strom	2.85%	0.82
Produzent - Strom und anderes	4.07%	0.55
Messstellenbetreiber - nur Strom	4.88%	0.77
Messstellenbetreiber - Strom und anderes	8.13%	0.59

Abbildung 63: Korrelation der Maturität mit OT-Auslagerung an Dritte

Verwendung von Cloud-Dienstleistern

Rund 1/3 (32.52%) aller Teilnehmer verwenden bisher IT Cloud-Dienstleister oder planen in naher Zukunft dies zu tun. Die durchschnittliche Maturität der IT-Sicherheit beläuft sich entweder auf 0.88 im Falle keiner Verwendung von Cloud-Dienstleistern, und auf 0.79 bei der (künftigen) Verwendung von Cloud-Dienstleitern. Es ist daher keine nennenswerte Korrelation erkennbar mit der aktuellen Maturität im Bereich der IT-Sicherheit, welches ebenso durch die Kolorierung visuell bestätigt wird. Es ist zudem anzumerken, dass die Prozentangaben in der Abbildung sich nicht auf sich nicht auf die Unternehmenstypen beziehen, sondern auf die Gesamtmenge der befragten Teilnehmer.

	Clouddienstleister sind bereits / werden in naher Zukunft für IT-Management verwendet	Durchn. Maturität - IT Sicherheit
Nein	**67.48%**	**0.88**
Netzbetreiber	32.93%	0.83
Produzent - nur Strom	3.66%	0.97
Produzent - Strom und anderes	9.76%	0.99
Messstellenbetreiber - nur Strom	5.28%	1.02
Messstellenbetreiber - Strom und anderes	15.85%	0.84
Ja	**32.52%**	**0.79**
Netzbetreiber	13.01%	0.78
Produzent - nur Strom	3.25%	0.48
Produzent - Strom und anderes	5.28%	0.86
Messstellenbetreiber - nur Strom	3.66%	0.96
Messstellenbetreiber - Strom und anderes	7.32%	0.81

Abbildung 64: Korrelation IT-Sicherheits-Maturität mit Verwendung von Cloud-Dienstleistern

Rund 10% aller Umfrage-Teilnehmer geben ebenfalls an gewisse Cloud-Dienstleistungen im Zusammenhang mit OT bereits in Anspruch zu nehmen oder in naher Zukunft damit zu planen. Hier lässt sich eine klare Korrelation erkennen mit Unternehmen, welche generell einen tieferen Wert betreffend OT-Sicherheit vorweisen. Die durchschnittliche Maturität der OT-Sicherheit beläuft sich entweder auf 0.9 im Falle keiner Verwendung von Cloud-Dienstleistern, und auf sehr tiefe 0.41 bei der (künftigen) Verwendung von Cloud-Dienstleitern. Die mehrheitlich stärkere grüne Farblichen (= höhere Maturitätswerte) der durchschnittenen Maturität bestätigt diese Beobachtung.

	Clouddienstleister sind bereits / werden in naher Zukunft für OT-Management verwendet	Durchn. Maturität - OT Sicherheit
Nein	**90.65%**	**0.90**
Netzbetreiber	41.46%	0.86
Produzent - nur Strom	5.69%	1.02
Produzent - Strom und anderes	13.82%	0.89
Messstellenbetreiber - nur Strom	7.72%	1.24
Messstellenbetreiber - Strom und anderes	21.95%	0.81
Ja	**9.35%**	**0.41**
Netzbetreiber	4.47%	0.41
Produzent - nur Strom	1.22%	0.44
Produzent - Strom und anderes	1.22%	0.04
Messstellenbetreiber - nur Strom	1.22%	0.73
Messstellenbetreiber - Strom und anderes	1.22%	0.42

Abbildung 65: Korrelation OT-Sicherheits-Maturität mit Verwendung von Cloud-Dienstleistern

Haltung betreffend Meldepflicht für Cyber-Vorfälle

Eine Mehrheit von 86 der 124 Umfrageteilnehmer (69%) begrüssen tendenziell die Einführung einer künftigen Meldepflicht für Cyber-Vorfälle. Von den 26 Unternehmen der Umfrage, welche ebenfalls bereits Mitglied des geschlossenen Kundenkreises von MELANI sind, begrüssen praktisch alle die Idee einer künftigen Meldepflicht. Zum Teil gaben aber selbst jene, welche diese Frage verneinten, im Kommentarfeld an, regelmässig die öffentlichen Informationen von MELANI zu beziehen. Lediglich ein Umfrageteilnehmer gab an, von MELANI vorher noch nichts gewusst zu haben.

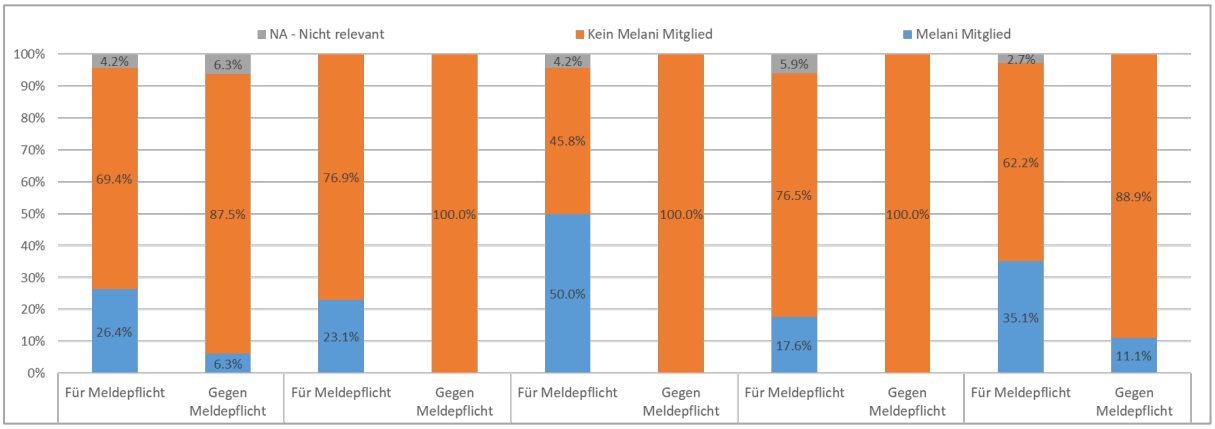


Abbildung 66: Korrelation der Maturität mit Einstellung zu einer Meldepflicht für Cyber-Vorfälle

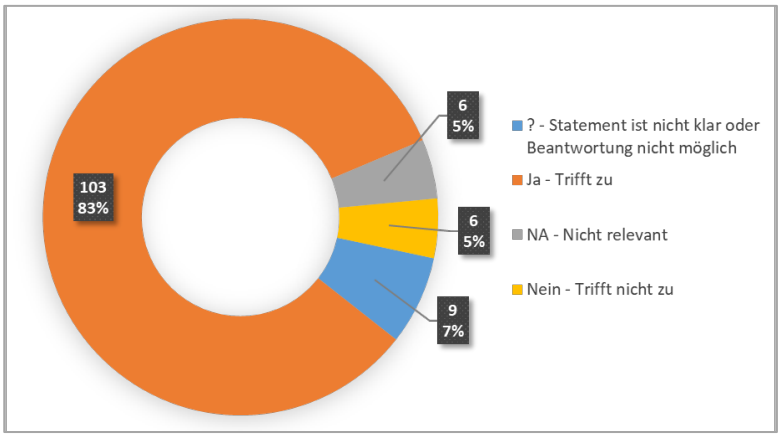
Die 26 Teilnehmer und Mitglieder des geschlossenen Kundenkreises von MELANI weisen im Schnitt ein höheres Maturitätsniveau aus (IT-Sicherheit = 1.11; OT-Sicherheit = 1.11). Nicht MELANI Mitglieder hingegen erreichen tiefer Maturitätsstufen (IT-Sicherheit = 0.76; OT-Sicherheit = 0.76). Dieser Umstand ist zu erwarten, da dies typischerweise Betriebe sind, welche ein eigenes SOC betreiben und so vor allem in der IKT-Funktion «Erkennen» gut aufgestellt sind. Zudem ermöglicht der Austausch mit MELANI einen besseren Wissensvorsprung, anhand von welchem sich die Unternehmen gezielt auf bestimmte Cyber-Bedrohungen vorbereiten können.

MELANI Mitgliedschaft relevant zu IT/OT Sicherheitsstand?	Netz-betreiber	Produzent - nur Strom	Produzent - Strom und anderes	Messstellenbetreiber - nur Strom	Messstellenbetreiber - Strom und anderes	Total
MELANI Mitglied						
Durchschn. Maturität - IT Sicherheit	1.09	1.06	1.23	0.87	1.10	**1.11**
Durchschn. Maturität - OT Sicherheit	1.11	1.36	1.10	1.20	1.04	**1.11**
Nicht MELANI Mitglied						
Durchschn. Maturität - IT Sicherheit	0.74	0.70	0.75	0.89	0.74	**0.76**
Durchschn. Maturität - OT Sicherheit	0.75	0.88	0.67	0.95	0.73	**0.76**

Abbildung 67: Korrelation der Maturität mit MELANI Mitgliedschaft

Berücksichtigung von Cyber-Sicherheit bei «Smart Meter»

Die Mehrheit, 83%, aller Umfrageteilnehmer bestätigte, dass Cyber-Sicherheitsaspekte bei der gesetzlichen Einführung von Smart Metern in die bestehende Unternehmensarchitektur mitberücksichtigt werden. Es besteht zudem eine deutlich positive Korrelation mit dem Reifegrad dieser Teilnehmer betreffend IT- / OT-Sicherheit. Dies ist begrüssenswert, zeigt sich doch, dass die Vorgaben der Stromversorgungsverordnung vom 2. November 2017 insgesamt einen positiven Effekt für die Digitalisierung und die Sicherheit entfalten in Bereich, die nicht direkt von den Vorgaben tangiert sind. Die Verordnung verlangt derweil, dass Schweizer Netzbetreiber bis 2027 80% der konventionellen Stromzähler durch diese kommunikationsfähigen Modelle ersetzt werden müssen. Es ist also zu erwarten, dass die Einführung der intelligenten Messsysteme eine insgesamt positive Wirkung quasi als «Windfall-Profit» auf die unternehmensseitige IT-/OT-Sicherheit. Die sättige grüne Einfärbung bei den JA-Antworten bestätigt dies zudem auch noch visuell.



	Durchschn. Maturität - IT Sicherheit	Durchschn. Maturität - OT Sicherheit
? - Statement ist nicht klar oder Beantwortung nicht möglich	0.57	0.60
Ja - Trifft zu	0.94	1.17
NA - Nicht relevant	0.11	0.19
Nein - Trifft nicht zu	0.36	0.45

Abbildung 68: Korrelation Maturität mit Berücksichtigung von Cyber-Sicherheitsaspekten bei der Einführung von Smart Metern

Organisatorische Verantwortung für IT-/OT-Sicherheit

Für Unternehmen bei welchen die Gesamtverantwortung für Cyber-Sicherheit beim Leiter IT liegen fielen die angegebenen Maturitätswerte im Schnitt höher aus (IT-Sicherheit = 1.09; OT-Sicherheit = 0.9). Umgekehrt haben Unternehmen, bei welcher die Gesamtverantwortung dem Leiter Produktion (= näher an OT) zugeteilt ist, im Schnitt eher tiefere Werte. Auch fielen Werte deutlich höher aus, wenn das obere Kader die Gesamtverantwortung trägt (IT-Sicherheit = 1.26; OT-Sicherheit = 1.49). Dies bedeutet nicht, dass diese Positionen über die nötigen Fachkenntnisse der Cyber-Fähigkeiten besitzen, sondern dass Cyber-Risiken auch als Chefsache wahrgenommen werden. Entsprechend verschieben sich die Verantwortlichkeiten für das Management der Risiken, da die entsprechende Rechenschaftspflicht innerhalb der Unternehmung eingesetzt wird.

Hoch sind die Maturitätswerte auch (IT-Sicherheit = 1; OT-Sicherheit = 0.99), wenn ein CISO für die Cyber-Sicherheit zuständig ist, welches darauf zurückgeführt werden kann, dass eine solche Rolle spezifisch zur Sicherung der Informationssicherheit institutionalisiert wurde.

Die Maturitätswerte bei jenen Unternehmen, welche diese Rolle nicht klar definiert haben, fallen wenig überraschend sehr tief aus (IT-Sicherheit = 0.37; OT-Sicherheit = 0.41). Die Cyber-Risiken kaum verwaltet. Entsprechend sind Risikomanagementprozesse und organisatorische Vorgaben zur IKT-Sicherheit nicht formalisiert.

Leiter IT		
	Durchschn. Maturität - IT Sicherheit	**Durchschn. Maturität - OT Sicherheit**
Nein	0.66	0.73
Ja	1.09	0.90
Leiter Produktion		
	Durchschn. Maturität - IT Sicherheit	**Durchschn. Maturität - OT Sicherheit**
Nein	0.86	0.83
Ja	0.45	0.00
Leiter Netz		
	Durchschn. Maturität - IT Sicherheit	**Durchschn. Maturität - OT Sicherheit**
Nein	0.84	0.77
Ja	0.89	0.93
CISO		
	Durchschn. Maturität - IT Sicherheit	**Durchschn. Maturität - OT Sicherheit**
Nein	0.81	0.76
Ja	1.00	0.99

CEO / Vorstand / Geschäftsleitung / Präsident

	Durchschn. Maturität - IT Sicherheit	Durchschn. Maturität - OT Sicherheit
Nein	0.79	0.70
Ja	1.26	1.49

Hersteller

	Durchschn. Maturität - IT Sicherheit	Durchschn. Maturität - OT Sicherheit
Nein	0.87	0.83
Ja	0.49	0.00

Externe Dienstleister

	Durchschn. Maturität - IT Sicherheit	Durchschn. Maturität - OT Sicherheit
Nein	0.83	0.80
Ja	1.17	0.82

Nicht klar definiert

	Durchschn. Maturität - IT Sicherheit	Durchschn. Maturität - OT Sicherheit
Nein	0.98	0.90
Ja	0.37	0.41

Abbildung 69: Korrelation Maturität mit Gesamtverantwortung für Cyber-Sicherheit

Anhang 2: Handlungsfelder der NCS 2018-2022

Handlungsfeld	Massnahmen
Kompetenzen- und Wissensaufbau	1. Früherkennung von Trends und Technologien und Wissensaufbau 2. Ausbau und Förderung von Forschungs- und Bildungskompetenz 3. Schaffung von günstigen Rahmenbedingungen für eine innovative IKT-Sicherheitswirtschaft in der Schweiz
Bedrohungslage	4. Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage
Resilienz-Management	5. Verbesserung der IKT-Resilienz der kritischen Infrastrukturen 6. Verbesserung der IKT-Resilienz in der Bundesverwaltung 7. Erfahrungsaustausch und Schaffung von Grundlagen zur Verbesserung der IKT-Resilienz in den Kantonen
Standardisierung / Regulierung	8. Evaluierung und Einführung von Minimalstandards 9. Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung 10. Globale Internet-Gouvernanz 11. Aufbau von Expertise zu Fragen der Standardisierung in Bezug auf Cyber-Sicherheit
Vorfallbewältigung	12. Ausbau von MELANI als Public-Private-Partnership für die Betreiber kritischer Infrastrukturen 13. Aufbau von Dienstleistungen für alle Unternehmen 14. Zusammenarbeit des Bundes mit relevanten Stellen und Kompetenzzentren 15. Prozesse und Grundlagen der Vorfallbewältigung des Bundes
Krisenmanagement	16. Integration der zuständigen Fachstellen aus dem Bereich Cyber-Sicherheit in die Krisenstäbe des Bundes 17. Gemeinsame Übungen zum Krisenmanagement
Strafverfolgung	18. Lagebild Cyber-Kriminalität 19. Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung 20. Ausbildung 21. Zentralstelle Cyber-Kriminalität
Cyber-Defence	22. Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution 23. Fähigkeit zur Durchführung von aktiven Massnahmen im Cyber-Raum gemäss NDG und MG 24. Gewährleistung Einsatzbereitschaft der Armee über alle Lagen im Cyber-Raum und Regelung ihrer subsidiären Rolle zur Unterstützung der zivilen Behörden
Aktive Positionierung der Schweiz in der internationalen Cyber-Sicherheitspolitik	25. Aktive Mitgestaltung und Teilnahme an Prozessen der Cyber-Aussensicherheitspolitik 26. Internationale Kooperation zum Auf- und Ausbau von Kapazitäten im Bereich Cyber-Sicherheit 27. Bilaterale politische Konsultationen und multilaterale Dialoge zu Cyber-Aussensicherheitspolitik
Aussenwirkung und Sensibilisierung	28. Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS 29. Sensibilisierung der Öffentlichkeit für Cyber-Risiken (Awareness)

Abbildung 70: Handlungsfelder und Massnahmen der NCS 2018-2022

Anhang 3: Risiko- und Schutzbedarfsanalysen

Dieser Anhang führ drei relevante Risiko- und Schutzbedarfsanalysen, welche im Rahmen der SKI und NCS durchgeführt wurden und in Kapitel 1.2.2 Bestehende Vorgaben Bezug genommen wurde.

Risiko- und Schutzbedarfsanalyse für Smart Grids (2016a)

Herausgeber: BFE, OFFIS – Institut für Informatik, Josef Ressel Zentrum FH Salzburg & ecofys

Die Schutz- und Sicherheitsanalyse wurde im Rahmen der Entwicklung von Smart Grids mit Fokus auf Flexibilitäten an der Schnittstelle Markt und Netz in der Schweiz vom BFE und anderen Auftragnehmern erstellet. Die Studie bietet allgemeine Massnahmen und Empfehlungen zu IT-Sicherheit, die sich im Kontext von Smart Grids ergeben. Diese umfassen unter anderem die folgenden Dimensionen: Prüfung und Verantwortlichkeit für das Informationssicherheitsmanagementsystem (ISMS) der kritischen Infrastruktur, Massnahmen zur Absicherung der Smart Grid Informationssysteme und der dazugehörigen Kommunikation und Massnahmen zur Sicherstellung der Integrität der Daten von Energieinformationssystemen und Nachrichten.

In diesem Studienprojekt wurde NISTIR 7628 als fachliches, logisches Referenzmodell zur Risikoanalyse genutzt. Das NISTIR 7628 bietet eine etablierte Basis, den Schutz einzelner Systeme und ihrer Schnittstellen zu ermitteln und später in eine Gesamtrisikobewertung einfliessen zu lassen.

Diese Analyse wird momentan für Revision StromVG herangezogen werden, damit, analog zum Smart Meter, sicherheitstechnische Anforderungen und Prüfverfahren erstellt werden können. Abermals, ist dieses Vorgehen durch die NCS Massnahme 8 bestätigt. Die Erarbeitung eines neuen Standards für Smart Grids muss jedoch insofern hinterfragt werden, da es bereits zahlreiche Initiativen gibt und die Gefahr besteht, die Übersicht über die verschiedenen Massnahmen der Teilbereiche zu verlieren womit die gesamtheitlichen Anforderungen der Cyber-Sicherheit gewissermassen verwässert werden.

Risiko- und Schutzbedarfsanalyse für Smart Meter (2016b)

Herausgeber: BFE & AWK Group

Konkret empfiehlt die Analyse einen Hersteller- und Produktorientierten Ansatz bei der Entwicklung von IKT-Sicherheitsanforderungen. Der Hersteller soll demnach gänzlich anhand eines Prüfmechanismus in die Verantwortung für IKT-Sicherheit gezogen werden. Netzbetreiber und Hersteller sollten diesen Standard gemeinsam und auf Basis einer durch das BFE und AWK Group erarbeiteten Risiko- und Schutzbedarfsanalyse insofern festlegen, dass der Standard durch bezeichnete Stellen für die intelligenten Messsysteme geprüft werden kann.

Diese Analyse wird derzeit von der Branche genutzt, um sicherheitstechnische Anforderungen und Prüfverfahren für Smart Meter zu definieren. Dieses Vorgehen ist durch die NCS 2018-2022 bestärkt, da wie in Massnahme 8 definiert, auditierbare IKT-Minimalstandards auf der Basis der durchgeführten Risiko- und Verwundbarkeitsanalysen evaluiert und eingeführt werden sollen.

Risiko- und Verwundbarkeitsanalyse des Teilsektors Stromversorgung (2017)

Herausgeber: BWL

Die Analyse betreffend kritischer Teilsektor Strom machte unter anderem die folgenden Erkenntnisse:

- Entlang der gesamten Versorgungskette ist die Produktion von Strom in den Kraft- und Unterwerken heute weniger stark verwundbar hinsichtlich ICT-Gefährdungen als der Betrieb der Verteil- und Übertragungsnetze.
- Der Betrieb der Leitungsnetze erfolgt heute dezentral und wird weitgehend durch digitale Systeme überwacht und teilweise gesteuert. Der Betrieb der Netze ist deswegen stärker verwundbar gegenüber IKT-Gefährdungen als die eigentliche Stromproduktion. In diesem Bereich sind die SCADA-Systeme von besonderer Bedeutung.
- Mit dem Einbau von Smart Metern und Smart Grid-Geräten wird das Schweizer Leitungsnetz steigt die Vernetzung. Dies bietet Vorteile in der Effizienz für den Betrieb der Leitungsnetze, schafft aber neue IKT-Verwundbarkeiten.
- Insgesamt wird die IKT-Verwundbarkeit der Stromversorgung in Zukunft weiter zunehmen.

Der gesamte Bericht ist nicht für die Öffentlichkeit zugänglich. Lediglich ein Factsheet fasst die Beurteilungen grob zusammen. Diese Beobachtungen sollten jedoch unbedingt bei der Erarbeitung eines gesamtheitlichen Standards berücksichtigt werden, damit die Anforderungen die identifizierten Risiken und Verwundbarkeiten angeglichen werden können.

Anhang 4: Existierende Branchenrichtlinien

Dieser Anhang listet die restlichen unverbindlichen Empfehlungen betreffend Cyber-Sicherheit für Strommarktteilnehmer auf, welche in Kapitel 1.2.2 Bestehende Vorgaben referenziert wurden.

All diese Dokumente sind, bis auf bestimmte Teile der Richtlinien für die Datensicherheit von intelligenten Messsystemen, freiwillig.

Richtlinien für die Datensicherheit von intelligenten Messsystemen für Zertifizierung und Betrieb von intelligenten Messsysteme (2018)

Herausgeber: VSE

Diese Branchenrichtlinie besteht aus zwei Teilen.

Einerseits wurde eine Zertifizierung für intelligenten Messsysteme eingeführt. Basierend auf der vorgängigen Schutz- und Sicherheitsanalyse für Smart Meter (2016a) wurde in Art. 8b StromVV, welcher per 1. November 2017 eingesetzt wurde, bestimmt, dass nur Smart Meter verwendet werden dürfen, die vorgängig eine Datensicherheitsprüfung durchlaufen haben. Somit müssen sich die Hersteller von Smart Metern ihr Produkt bei einer akkreditierten Prüfstelle, der Konformitätsbewertungsstelle des Eidgenössischen Institut für Metrologie (METAS), zertifizieren lassen. Die Prüfmethodologie wurde durch den Verein Smart Grid Industrie Schweiz (Swissmig) publiziert.

Andererseits umfasst diese Branchenrichtlinie Vorgaben bezüglich dem Betrieb der Messsysteme durch die Unternehmen selbst. Dieser Teil der Branchenrichtlinie ist nicht verpflichtend und wird nicht geprüft, kann aber als unverbindlicher Standard betreffend Cyber-Sicherheit für diese Unternehmen verstanden werden.

Grundsätzlich sind die definierten Anforderungen eine gute Basis. Sie müssen aber zwingend mit weiteren Sicherheitsmassnahmen ergänzt werden, da der der alleinige Fokus auf Produktsicherheit zu begrenzt vor dem Hintergrund der aktuellen IKT-Bedrohungslage ist. Zudem ist der Inhalt auf die Datensicherheit aufgelegt und betrifft somit nur einen Teilbereich der Cyber-Sicherheit.

Standardisierter Datenaustausch für den Strommarkt Schweiz (2018)

Herausgeber: VSE

Diese Branchenempfehlung ist ein Teil des Rahmenwerks für den gesamtheitlichen Umgang mit Daten in der Energiebranche. Sie beschreibt Datenaustauschprozesse, die für die erste Stufe als auch für die vollständige Strommarktliberalisierung (Umsetzung Stromversorgungsgesetz, Energiegesetz und Verordnungen) notwendig sind. Insbesondere sind Messdatenaustausch, Wechselprozesse und deren Umsetzung beschrieben. Somit werden durch die vorliegenden Standards ein automatisierter Ablauf der Prozesse erlaubt.

Abermals ist hervorzuheben, dass die Datensicherheit nur einen Teilbereich der Cyber-Sicherheit abdeckt.

Data Policy in der Energiebranche (2019)

Herausgeber: VSE

Diese Branchenempfehlung ist ein Teil des Rahmenwerks für den gesamtheitlichen Umgang mit Daten in der Energiebranche. Das Dokument dient als Empfehlung für einen branchenweiten, geordneten und rechtskonformen Umgang mit Daten sowie als praxisnahe Data Policy für die Energiebranche. Diese umfasst Grundsätze für relevante Fragestellungen zu Daten-Nutzung, Daten-Compliance (d.h. Datenschutz, Datensicherheit) sowie Daten-Governance. Diese Grundsätze werden abgebildet in Form von Handlungsempfehlungen, Hilfsmitteln sowie organisatorischen Vorschlägen für datenrelevante Themen innerhalb eines mit der Energiebranche verbundenen Unternehmens.

Erneut ist zu betonten, dass die Datensicherheit nur mit einem Teilbereich der Cyber-Sicherheit befasst.

Anhang 5: Praxisbeispiele Frankreich und Deutschland

Dieser Anhang zeigt zwei Praxisbeispiele, Frankreich und Deutschland, wie die NIS-Richtlinie betreffend Stromsektor umgesetzt wurde auf. Dieser Vergleich mit den beiden Nachbarsländern wird gezogen, um konkrete Beispiele für mögliche weiterführende Herangehensweise betreffend Cyber-Sicherheit und Cyber-Resilienz Konzept für den Schweizer Strommarkt aufzuzeigen. Dies bedeutet nicht, dass diese direkt auf die Schweiz angewendet werden können, kann jedoch als generelle Orientierungshilfe verwendet werden.

Die nachfolgende Tabelle stellt Frankreich und Deutschland und deren jeweilige Implementierung der NIS-Richtlinie gegenüber. Zusätzlich zu den Kategorien, welche in der Tabelle aufgeführt werden, ist anzumerken, dass die nicht aufgelisteten Massnahmen der NIS-Richtlinie, also nationale Cyber-Sicherheit Strategie, Teilnahme im Kooperationsnetzwerk und CERT-Netzwerk, von beiden Ländern erfüllt wurde.

Tabelle 24: Vergleich betreffend Umsetzung der NIS-Richtlinie im Stromsektor in Frankreich und Deutschland

	Frankreich[108]	Deutschland[109]
Regulator Stromsektor und/oder nationale Cyber-Koordinationsstelle (SPoC)	Regulator und SPoC: Agence nationale de la sécurité des systèmes d'information (ANSSI)	Regulator: Bundesnetzagentur in Zusammenarbeit mit Bundesamt für Sicherheit in der Informationstechnik (BSI) SPoC: BSI
Art der Regulierung	Sektorübergreifend	Sektor-spezifisch
Von der Regulierung betroffen	Kritische Infrastrukturen (KI)	Strom- und Gasnetzte, sowie Energieanlagenbetreiber (die nach der BSI-Kritisverordnung als KI bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind)
Verbindliche Sicherheitsanforderungen	KI Betreiber mussten die eigenen kritischen Informationssysteme selbst identifizieren und eine Liste davon bei ANSII einreichen. Diese Systeme unterliegen technischen und organisatorischen Regeln, welche von ANSII vorgegeben sind. Diese Regeln sind an keinen spezifischen internationalen Standard geknüpft und gehen über die Anforderungen des NIST CSF Framework hinaus. Es musste auch ein betrieblicher Ansprechpartner gegenüber ANSII angegeben werden. Zusätzlich stellt ANSII «Sicherheit-Visa» für Produkte und Dienstleistungen aus, ohne welches KI-Unternehmen die Sicherheitslösungen nicht einsetzen dürfen.	IT-Sicherheitskataloge für Strom- und Gasnetzte, sowie & Energieanlagenbetreiber. Kernanliegen: Einführung eines ISMS nach ISO27001 mit Berücksichtigung von ISO27002 & ISO27019, sowie Schaffung eines Ansprechpartners für IKT-Sicherheit. *Entwicklung*: Neuer Sicherheitskatalog mit aktualisierten Anforderungen für alle Netze und Dienste ist momentan in Überarbeitung. Der Entwurf sieht insbesondere vor, dass kritische Komponenten zertifiziert werden und ein Nachweis der Vertrauenswürdigkeit von Herstellern und Lieferanten eingeholt wird. Zusätzlich sollen Betreiber von KI dazu verpflichtet werden, Systeme zur Angriffserkennung einzusetzen. Ein besonderer Fokus wird hierbei auf den Einsatz von Künstliche Intelligenz gesetzt, um allfällige Angriffs-Muster frühzeitig erkennen zu können.
Nachweise für die wirksame Umsetzung der Sicherheitsanforderungen	Die Prüfung kann von ANSSI oder einem qualifizierten Dienstleister («prestataires de service qualifiés») durchgeführt werden. Die Dienstleister werden hierfür von Comité français d'accréditation (COFRAC) akkreditiert und von ANSSI lizenziert.	Zertifizierung des betroffenen Betriebes nach IT-Sicherheitskatalog bei einer Prüfstelle, welche durch die Deutsche Akkreditierungsstelle (DAkkS) anhand eines Konformitätsbewertungsprogramm akkreditiert wurde. Nachweise der Zertifizierung sind bei der Bundesnetzagentur einzureichen.

108 Bird & Bird (2020), Developments on NIS Directive in EU Member States.
Agence nationale de la sécurité des systèmes d'information (2020), The French CIIP Framework.

109 Deutsche Akkreditierungsstelle (2020), Akkreditierung für IT-Sicherheitskatalog nach EnWG.
Deutsche Bundesnetzagentur (2020), IT-Sicherheit im Energiesektor.
Deutsches Bundesamt für Sicherheit in der Informationstechnik (2017), Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz.

Intervall der Überprüfung	Der Premierminister, basierend auf einer Konsultation mit den relevanten Ministern, kann eine Überprüfung der Einhaltung der Regeln entweder auf regulärer Basis (max. einmal pro Jahr) oder nach einem Vorfall auslösen.	Nachweise für Einhaltung des IT-Sicherheitskatalog sind alle zwei Jahre einzureichen.
Meldepflicht	Störungen, welche wahrscheinlich grosse Auswirkungen auf die Funktionsfähigkeit der kritischen Infrastrukturen hat, müssen unverzüglich von dem betroffenen Unternehmen an ANSSI gemeldet werden. Es wurden Sektor-spezifische Anforderungen gestellt, welche aber im Rahmen dieses Berichts für den Stromsektor nicht identifiziert werden konnten.	Betreiber von KI haben folgende Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden: - Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen geführt haben, - erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können. Eine eindeutige, umfassend geltende Antwort, wann eine Störung erheblich ist, ist nicht möglich. Stattdessen ist es erforderlich, dass die Verantwortlichen der kritischen Infrastruktur Einzelfallentscheidungen treffen.
Bestrafung bei Nichteinhaltung	Geldstrafe von bis zu 100’000 Euro bei mangelnder Implementierung der Sicherheitsanforderungen. Geldstrafe von bis zu 50’000 Euro bei Nichteinhaltung der Meldepflicht.	Geldstrafe von bis zu 100’000 Euro bei mangelnder Implementierung der Sicherheitsanforderungen. Geldstrafe von bis zu 50’000 Euro bei Nichteinhaltung der Meldepflicht.

Die Tabelle zeigt auf, dass die beiden EU-Länder die NIS-Richtlinie teilweise sehr unterschiedlich umgesetzt haben. Es vier grundlegende Differenzen in der Auslegung der Anforderungen identifiziert.

Erstens, sind die Zuständigkeiten für Cyber-Sicherheit unterschiedlich geregelt. In Frankreich ist primär das ANSSI für den Bereich der Cyber-Sicherheit zuständig. Zwar werden gewisse Regelungen mit anderen staatlichen Behörden geregelt, jedoch ist das System stark zentralisiert und auf ANSII als dominante Cyber-Behörde ausgerichtet. ANSSI legt die IKT-Richtlinien fest, sowie regelt die Überprüfung der Nachweise. In Deutschland wurden die Sicherheitsanforderungen in Zusammenarbeit des BSI mit der Bundesnetzagentur erarbeitet, aber schliesslich ist die Bundesnetzagentur für die Regulierung zuständig. Zudem sind die Nachweise bei der Bundesnetzagentur einzureichen.

Zweitens, betreffend Kategorisierung der Sicherheitsanforderungen ist anzumerken, dass Frankreich eine sektorübergreifende- und Deutschland eine Sektor-spezifische-Regelung veranlasst haben. Ein

sektorübergreifender Typ bedeutet, dass generell die gleichen Cyber-Sicherheit Anforderungen an alle KI gestellt werden. In Frankreich wurden allgemein gültige Regeln aufgestellt, welche keine Sektor-spezifischen Massnahmen festlegen. Die von ANSSI vorgegebenen Verpflichtungen sind für jeden KI Betrieb gleichermassen gültig. Es ist jedoch anzumerken, dass bei der Implementierung die Forderungen an die Gegebenheiten der Betriebe angepasst werden können, diese aber innerhalb der vorbestimmten Kategorien durchgeführt werden, sowie gemäss risikobasierten Grundsatz angemessen sein müssen. In Deutschland hingegen sind die Cyber-Sicherheit Anforderungen an die unterschiedlichen Sektoren angepasst. Die IT-Sicherheitskataloge sind auf die sektoriellen Umstände der Unternehmen angepasst und geben konkrete Massnahmen vor, wie diese zu berücksichtigen sind.

Drittens, sind die Sicherheitsanforderungen entsprechend verschieden definiert. In Deutschland sind die ISO-Standards massgebend in den IT-Sicherheitskatalogen verankert, wobei in Frankreich die Regeln keine international anerkannten Sicherheitsstandards erwähnen. Das ANSSI hat eigene Anforderungen aufgestellt, welche sich zwar stark mit den Vorgaben in den ISO-Standards überschneiden, diese anerkennt diese aber nicht explizit.

Letztlich, ist das Einholen der Nachweise für die Einhaltung der Sicherheitsanforderungen bei den betroffenen Betrieben unterschiedlich festgelegt. In Deutschland wurde basierend auf einem von dem DAkkS durchgeführten Konformitätsprogramm gewisse externe Prüfstellen akkreditiert, damit diese unabhängig von der Bundesnetzagentur oder BSI Zertifizierungen nach dem IT-Sicherheitskatalog ausstellen können. Diese Zertifizierungen müssen zwar von dem geprüften Unternehmen und dem Prüfer bei der Bundesnetzagentur eingereicht werden, jedoch ist der Prüfung der Nachweise für die Einhaltung der Sicherheitsanforderungen stark dezentralisiert worden. In Frankreich ist dieser Akkreditierungsmechanismus ebenso eingeführt worden, ist aber nicht weniger stark dezentralisiert, da ANSSI oder ein qualifizierter Dienstleister die Prüfung durchführen kann.

Unabhängig von diesen zahlreichen Unterschieden, wurden aber auch gewisse Gemeinsamkeiten identifiziert. Die Meldepflicht, sowie die Bestrafungsmechanismen sind in Frankreich und Deutschland sehr ähnlich geregelt. In beiden Ländern ist die Meldepflicht an Sektor-spezifische Kriterien angepasst und muss an die zentrale Cyber-Sicherheit Behörde, resp. ANSSI oder BSI, gemeldet werden. Weiter belaufen sich die Geldstrafen bei einer Nichteinhaltung der Sicherheitsanforderungen oder der Meldepflicht auf die gleichen monetären Beträge. Schliesslich, scheint Deutschland sich auch bei der momentanen Überarbeitung der IT-Sicherheitskataloge an die Massnahme Frankreichs «Sicherheit-Visa» für Produkte und Dienstleitungen auszustellen, anzunähern. Dies ist im Rahmen des «EU Cybersecurity Act» zu verstehen, welcher ein EU-weit geltendes Rahmenwerk für die IKT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen etabliert.