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.

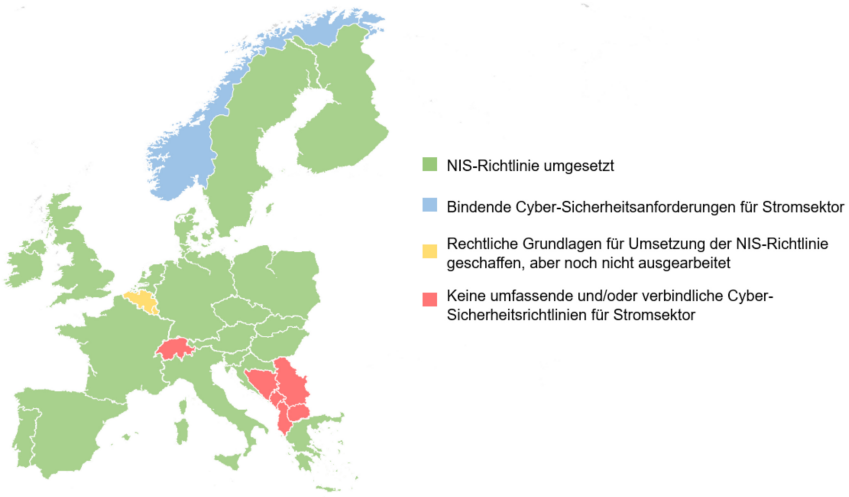

Abbildung MS 1: Europäischer Vergleich betreffend bindenden Sicherheitsanforderungen und Meldepflichten[1]

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.

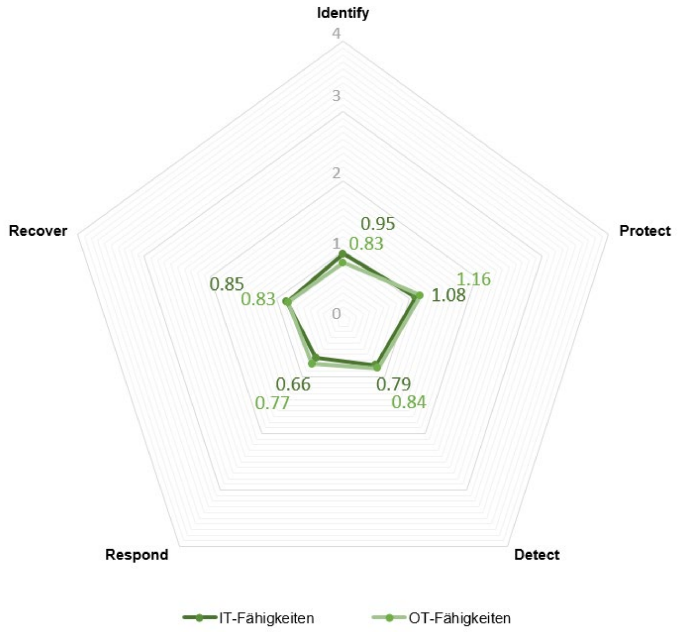

Abbildung MS 2: Durchschn. IKT Maturitätsstand des Schweizer Stromsektors – «E-Survey» Resultate 2020

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.