Gesetzes-empfehlung

Ein Vorschlag zur Verbesserung der Cybersicherheit kritischer Infrastrukturen in der Schweiz

Warum diese Gesetzesempfehlung?

Auch wenn in der Schweiz allmählich ein rechtlicher Rahmen für Cybersicherheit entwickelt wird, bestehen immer noch erhebliche rechtliche Lücken. Das neue Informationssicherheitsgesetz (ISG) ist ein notwendiger, aber kein hinreichender Schritt, um die Widerstandsfähigkeit des Landes gegenüber Cyber-Bedrohungen zu verbessern.

Dieses Dokument zeigt die wichtigsten rechtlichen Lücken auf, wobei der Fokus auf kritische Infrastrukturen liegt. Es skizziert einen Vorschlag, wie durch gesetzgeberische Massnahmen Anreize geschaffen werden können, um verbindliche Mindestanforderungen an die Cybersicherheit für kritische Infrastrukturen einzuführen.

Dieser Vorschlag ist das Ergebnis des Forschungsprojekts «Creating an ethical and legal governance framework for trustworthy cybersecurity in Switzerland», das im Rahmen des Nationalen Forschungsprogramms 77 «Digitale Transformation» von Forschern der Universität Zürich und der Universität Lausanne mit Unterstützung des Schweizerischen Nationalen Zentrums für Cybersicherheit durchgeführt wurde.

Zentrale Begriffe und Grundproblem

Was ist Cybersicherheit?

Cybersicherheit kann definiert werden als die Gesamtheit aller Massnahmen, die der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen[1].

Der Begriff der Cybersicherheit kann von jenem der «Informationssicherheit» und der «IT-Sicherheit» unterschieden werden. Allerdings ähneln Massnahmen der Cybersicherheit weitgehend den Massnahmen zur Gewährleistung der Informations- und IT-Sicherheit und können daher mit diesen kombiniert werden. Die drei Begriffe sind eng miteinander verknüpft.

Cybersicherheit ist eine globale Herausforderung und kann nicht als ein Problem verstanden werden, das mit rein technischen Mitteln gelöst wird. Vielmehr umfasst sie verschiedene Dimensionen, einschliesslich Gesetzgebung und Regulierung.

In der Vergangenheit wurden verschiedene Rechtsbereiche unter Berücksichtigung von Erwägungen geregelt, die an die Cybersicherheit grenzen: Das Strafrecht befasst sich beispielsweise mit Cyberkriminalität; Fragen der Cyberverteidigung fallen in den militärischen

1 Bundesrat, Nationale Cyber-Strategie (NCS), 2023, S. 9. Die NCS wurde 2023 verabschiedet. Sie ist die Strategie zum Schutz der Schweiz vor Cyberbedrohungen und ersetzt die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken von 2018–2022.

77 NFP Digitale Transformation Nationales Forschungsprogramm
Universität Zürich[UZH]
UNIL | Université de Lausanne

Bereich; Cybersicherheitsanforderungen betreffen oft nur bestimmte Industriezweige. Diese Heterogenität macht es schwierig, Cybersicherheit zu regeln.

Was sind kritische Infrastrukturen?

Kritische Infrastrukturen sind Prozesse, Systeme und Einrichtungen, die für das Wohlergehen der Bevölkerung und der Volkswirtschaft wesentlich sind (Art. 5 lit. c ISG). Derzeit gibt es keine genaue gesetzliche Definition des Begriffs «kritische Infrastruktur». Art. 5 lit. c ISG ergänzt lediglich den Begriff um einige Beispiele wie «Trinkwasser- und Energieversorgung, Informations-, Kommunikations- und Transporteinrichtungen».

Zu den kritischen Infrastrukturen zählen Organisationen, die für die Volkswirtschaft und das Wohlergehen der Bevölkerung notwendig sind. Die nationale Strategie zum Schutz kritischer Infrastrukturen betrachtet alle «Elemente» als kritische Infrastrukturen, die Leistungen in einem der 27 kritischen Teilsektoren erbringen, aus denen sich die 9 anerkannten kritischen Sektoren der Schweiz zusammensetzen, wobei das ISG dies nicht weiter spezifiziert[2]. Dazu gehören kleine, mittlere und grosse Unternehmen sowieselbstverwaltete und staatliche Organisationen.

Warum ist es wichtig, die Cybersicherheit für kritische Infrastrukturen zu regeln?

Aufgrund der vielen Aspekte und unterschiedlichen Rechtsbereiche, die sich mit Fragen der Cybersicherheit befassen, ist es derzeit nicht möglich, eine einzige und zentrale Cybersicherheitsregelung für die gesamte Bevölkerung zu schaffen. Daher sollte der Schwerpunkt auf der Regulierung der Cybersicherheit für Organisationen liegen, die für das Wohlergehen der Bevölkerung oder für die nationale Wirtschaft wesentlich sind. Regulierung ist ein notwendiger Anreiz für die Betreiber kritischer Infrastrukturen, ihre Widerstandsfähigkeit bei Cybervorfällen zu verbessern.

In der Schweiz entsteht allmählich ein rechtlicher Rahmen, um einige Betreiber kritischer Infrastrukturen dazu anzuhalten, ein angemessenes Niveau der Cybersicherheit zu gewährleisten und über gewisse Fähigkeiten zur Bewältigung von Cybervorfällen zu verfügen. Diese Bemühungen reichen unserer Ansicht nach jedoch nicht aus, da immer noch Lücken bestehen. Viele kritische Infrastrukturen unterliegen keinen Mindestanforderungen an die Cybersicherheit. Darüber hinaus ist es für viele Organisationen schwierig herauszufinden, ob sie nun kritische Infrastrukturen sind oder ob sie entsprechenden Anforderungen unterliegen sollen. Dies ist problematisch.

Ein gesetzlicher Rahmen im Aufbau

Der aktuelle Rechtsrahmen für Cybersicherheit kritischer Infrastrukturen

Die Cybersicherheit ist ein wachsender Bereich, für den die Regulierungsbemühungen erst vor kurzem begonnen haben.

Das wichtigste Gesetz in diesem Bereich ist das Informationssicherheitsgesetz (ISG). Das ISG wird zusammen mit vier Verordnungen am 1. Januar 2024 in Kraft treten. Es führt insbesondere verbindliche Mindestanforderungen an die Informationssicherheit und die IT-Sicherheit für Behörden und Organisationen des Bundes ein. Die Bestimmungen des ISG halten Behörden und Organisationen des Bundes dazu an, technische und organisatorische Massnahmen zur Verbesserung der Cybersicherheit in ihrer Organisation umzusetzen.

Das ISG wurde kürzlich überarbeitet, um eine Verpflichtung für kritische Infrastrukturen einzuführen, Cyberangriffe zu melden. Das überarbeitete ISG (ISG2) soll 2025 in Kraft treten.

Obwohl das ISG einen wichtigen Schritt darstellt, ist es noch zu begrenzt. Viele andere kritische Infrastrukturen könnten von den Massnahmen, die das ISG vorschreibt, profitieren.

Parallel zum ISG überarbeiten einige kritische Subsektoren wie die Stromversorgung derzeit ihre Gesetze, um verbindliche Mindestanforderungen an die Cybersicherheit einzuführen. Das Stromversorgungsgesetz (StromVG) und die dazugehörige Verordnung werden derzeit geändert, da die gesetzlichen Grundlagen für die Verbesserung der Cyber-Resilienz kritischer Infrastrukturen in der Stromversorgung fehlen.

Darüber hinaus gibt es gesetzliche Bestimmungen zu Geheimnissen (z.B. zu Geschäftsgeheimnissen) oder zum Datenschutz, die Überlegungen zur Cybersicherheit für kritische Infrastrukturen und im weiteren Sinne vorsehen. Zu diesen Gesetzen gehört insbesondere das Datenschutzgesetz (DSG).

Schliesslich ermöglichen vertragliche, zivil-, verwaltungs- oder strafrechtliche Haftungsbestimmungen zumindest im Nachhinein eine Wiedergutmachung für bestimmte Mängel im Bereich der Cybersicherheit.

2 Zu den 9 Sektoren zählen Behörden, Energie, Entsorgung, Ernährung, Finanzen, Gesundheit, Information und Kommunikation, öffentliche Sicherheit und Verkehr, vgl. Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen vom 16. Juni 2023 (BBI 2023 1659, S. 7).

Lücken im gesetzlichen Rahmen

Wir sind erstens der Ansicht, dass das Fehlen eines minimalen und harmonisierten Niveaus von Cybersicherheit mit der Schwierigkeit in Verbindung gebracht werden muss, den Begriff der kritischen Infrastruktur zu verstehen. Es fehlt mit anderen Worten eine klarere juristische Definition dieses Begriffs.

Zweitens gibt es für viele kritische Infrastrukturen keine oder nur lückenhafte Mindestanforderungen an die Cybersicherheit. Zum Beispiel:

1. Die Spitäler unterliegen der Meldepflicht von Cyberangriffen. Sie sind gesetzlich verpflichtet, Cybersicherheit unter besonderen Umständen zu gewährleisten, typischerweise wenn es um den Einsatz medizinischer Geräte oder um die Sicherheit der Arbeit mit elektronischen Patientenakten geht. Für den Rest ihrer IT-Infrastruktur gelten aber für Krankenhäuser keine verbindlichen Mindestanforderungen, sondern nur Empfehlungen. Auch wenn einige Krankenhäuser über interne Prozesse zur Gewährleistung der Cybersicherheit verfügen, ist dies nicht bei allen der Fall.

2. Die kommunalen Behörden unterliegen lediglich der Meldepflicht von Cyberangriffen. Ansonsten hängen die minimalen Anforderungen an die Cybersicherheit vom Kanton oder von den internen Weisungen der Gemeinde ab, was keinen ausreichenden Anreiz für eine angemessene Cyber-Resilienz ist.

3. Der Teilsektor «IT-Dienstleistungen» umfasst alle IT-Dienstleistungen für die Wirtschaft, insbesondere die Verarbeitung und Speicherung von Daten, IT-Sicherheitsdienste oder Cloud-Dienste. Die in diesem Teilsektor tätigen Organisationen unterliegen keinen Mindestanforderungen an die Cybersicherheit, sei es für die von ihnen verarbeiteten Informationen und die von ihnen genutzten IT-Ressourcen oder für die Dienstleistungen und Produkte, die sie ihren Kunden anbieten oder zur Verfügung stellen. Die bestehenden Regelungen zur Abwehr von Cyberangriffen auf Personen, zum Datenschutz, zur vertraglichen Haftung oder zur Produktsicherheit haben nur eine begrenzte Reichweite und sind rein reaktiver und nicht präventiver Natur.

Drittens zeigt sich, dass viele Betreiber Schwierigkeiten haben, sich in der Vielfalt der für sie geltenden Bestimmungen zurechtzufinden, da diese Bestimmungen im Normenkorpus verstreut sind und die Betreiber nicht verpflichtet sind, eine Liste der für ihre Tätigkeit geltenden Normen zu erstellen. Daher mangelt es dem aktuellen Rechtsrahmen an Kohärenz.

Die Lösung: übergreifende Mindestanforderungen

Heutzutage sind übergreifende und für alle kritischen Infrastrukturen geltende Mindestanforderungen erforderlich. Dies muss durch ein allgemeines Gesetz geschehen

Wir plädieren für die Einführung von Mindestanforderungen, die für alle kritischen Infrastrukturen gelten. Es ist wichtig, dass alle kritischen Infrastrukturen ihre Cyber-Resilienz verbessern. Der beste Weg, dieses harmonisierte Niveau zu erreichen, ist die Anwendung von Mindestanforderungen an die Cybersicherheit auf alle diese Organisationen (mit Ausnahme der weniger wichtigen)[3].

Die Gründe für eine allgemeine Gesetzgebung sind folgende.

- Eine allgemeine Rechtsgrundlage sorgt für mehr Klarheit bei kritischen Infrastrukturen auch hinsichtlich der Frage, welche als solche zu gelten hat.
- Eine allgemeine Rechtsgrundlage würde für alle kritischen Infrastrukturen schneller in Kraft treten und eine bessere Anpassungsfähigkeit an technologische Entwicklungen ermöglichen.
- Durch einheitliche Anforderungen kann verhindert werden, dass bestimmte Organisationen von den Bemühungen anderer Organisationen profitieren, indem sie sich nicht ausreichend engagieren (z.B. aufgrund von Kosteneinsparungen).
- Eine einheitliche Regelung verhindert zudem, dass bestimmte kritische Infrastrukturen durch die Maschen des Netzes fallen.
- Eine allgemeine Rechtsgrundlage kann leicht als Vorbild für die Wirtschaft als Ganzes dienen, die sich daran orientieren könnte.

Das Informationssicherheitsgesetz (ISG) ist der geeignete Ausgangspunkt für eine einheitlichere Regelung der Cybersicherheit

Das ISG ist das wichtigste Gesetz für die Cybersicherheit in der Schweiz. Die Verabschiedung des ISG und dessen Anpassung ist, wie dargelegt, ein wichtiger Schritt für eine Verbesserung der Cybersicherheit hierzulande. Das ISG dient bereits heute als Grundlage für Mindestanforderungen an die Informations- und IT-Sicherheit von Bundesbehörden und Organisationen und wird als

3 Dies im Gegensatz zu dem, was die NCS befürwortet, nämlich die laufende Überprüfung der gesetzlichen Bedürfnisse und die Anpassung des gesetzlichen Rahmens, Bundesrat, NCS, 2023, S. 21.

Rechtsgrundlage für die Meldepflicht von Cyber-Angriffen auf kritische Infrastrukturen dienen.

Das ISG ist daher geeignet, wenn nicht sogar ideal, um Mindestanforderungen an die Cybersicherheit einzuführen, die für alle kritischen Infrastrukturen gelten.

Unser legislativer Vorschlag

Unser Vorschlag für Mindestanforderungen für kritische Infrastrukturen

Unser Vorschlag besteht aus drei Verbesserungen des ISG:

1. ***Der Begriff der «kritischen Infrastrukturen» ist zu präzisieren und der Anwendungsbereich der Mindestanforderungen des ISG ist zu erweitern. Er sollte nicht auf Behörden und Organisationen des Bundes beschränkt sein, sondern für jede kritische Infrastruktur gelten.***

Der Begriff der kritischen Infrastrukturen muss im Vergleich zu dem, was Art. 5 lit. c ISG derzeit vorsieht, präzisiert werden. Das Gesetz kann den Hinweis der Strategie zum Schutz kritischer Infrastrukturen als Inspiration nehmen, um zu verdeutlichen, dass kritische Infrastrukturen neben der Notwendigkeit für die Volkswirtschaft und das Wohlergehen der Bevölkerung auch Elemente sind, die Leistungen in einem der kritischen Teilsektoren erbringen.

Der Anwendungsbereich der Mindestanforderungen hängt von der Definition kritischer Infrastrukturen ab. Denkbar wäre ein ähnlicher Anwendungsbereich wie in Art. 74b ff. ISG2 oder eine allgemeine Verpflichtung für alle kritischen Infrastrukturen, die Mindestanforderungen zu erfüllen, mit einer Ausnahme, die darin besteht, dass der Bundesrat bestimmte Organisationen ausnehmen kann (typischerweise aufgrund einer geringeren Bedeutung für die Wirtschaft oder das Wohlergehen der Bevölkerung), wie dies bereits in Art. 74c ISG2 der Fall ist.

2. ***Die Mindestanforderungen des ISG müssen verschärft werden.***

Die vom ISG und seiner Verordnung vorgeschriebenen Massnahmen decken bereits einen gewissen Bedarf ab. Darüber hinaus wären folgende Massnahmen denkbar: die Entwicklung von Plänen zur Bewältigung von Cybervorfällen, Inventare der zu schützenden Objekte oder allgemein anwendbare Normen für die Cybersicherheit sowie die Verpflichtung zu Cybersicherheit als Standard und «by design».

3. ***Weitere spezifische Anforderungen müssen im ISG enthalten sein und für digitale Sicherheitsdienste wie Computer Security Incident Response Teams (CSIRTs) gelten.***

CSIRT und IT-Dienste im Allgemeinen müssen nicht nur die Cybersicherheit der von ihnen verarbeiteten Informationen oder der von ihnen verwendeten IT-Werkzeuge gewährleisten, sondern auch die der von ihnen angebotenen Produkte und Dienste.

Diese Verpflichtung muss in Form einer Garantie für ausreichende Kapazitäten und Fähigkeiten (personell oder finanziell) konkretisiert werden. Es sollte auch eine Verpflichtung zur Gewährleistung der Cybersicherheit auf jeder Stufe der Lieferkette eines Produkts oder einer Dienstleistung bestehen. Ausserdem sollte eine Transparenzverpflichtung in Bezug auf die Qualität und Sicherheit der erbrachten Dienstleistungen bestehen.

Die Gesetzgebung muss Raum für Ausführungsbestimmungen lassen

Zusätzlich zu den vorgeschlagenen Änderungen im ISG müssen Ausführungsakte in Form von Verordnungen, Soft-Law sowie Technische und Administrative Vorschriften (TAV) verabschiedet werden können. Diese können präziser sein sowie schneller geändert und angepasst werden als ein Gesetz. Involvierte Behörden, die über weitergehende Kompetenzen verfügen (Bundesrat, Bundesamt für Cybersicherheit (BACS), Fachstelle des Bundes für Informationssicherheit[4], sektorielle Behörden und Berufsverbände).

Das neue BACS muss weiterhin über Kompetenzen für die Cybersicherheit bei kritischen Infrastrukturen verfügen. Die neu geschaffene Fachstelle des Bundes für Informationssicherheit wird wahrscheinlich über die Kompetenz verfügen, Richtlinien (hauptsächlich zuhanden des Bundes) zu erlassen, und es wird sich zeigen, wie diese Kompetenzen zwischen den beiden Behörden organisiert werden. So sollte das BACS beispielsweise befugt sein, Richtlinien und Leitlinien zu erlassen (wie die Richtlinie Si001 für den Bund, aber für andere kritische Infrastrukturen). In jedem Fall müssen die konkreten Massnahmen, die kritische Infrastrukturen ergreifen müssen, in der Regel in Durchführungsbestimmungen und nicht im Gesetz festgelegt werden.

Darüber hinaus stellen wir fest, dass die sektoralen Behörden und Berufsverbände mit den Organisationen, die

4 Die Fachstelle des Bundes für Informationssicherheit wird mit dem Inkrafttreten des ISG am 1. Januar 2024 geschaffen. Sie ist Teil des Staatssekretariats für Sicherheitspolitik (SEPOS) des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS). Ihre Aufgaben sind in Art. 83 ISG und in verschiedenen Bestimmungen der ISV beschrieben; für weitere Informationen, https://www.sepos.admin.ch/de

in bestimmten Teilsektoren tätig sind, besonders gut vertraut sind. Die Verabschiedung von Mindestanforderungen für alle Betreiber kritischer Infrastrukturen in einer zentralisierten Rechtsgrundlage (ISG) sollte die Verabschiedung weitergehender sektorspezifischer Regulierung, die sektorspezifische Merkmale oder Besonderheiten im Zusammenhang mit der Nutzung bestimmter Technologien berücksichtigen, deshalb nicht verhindern. So haben beispielsweise verschiedene Sektoren der wirtschaftlichen Versorgungskette auf der Grundlage der vom Bundesamt für wirtschaftliche Landesversorgung verabschiedeten Mindestnorm für Informations- und Kommunikationstechnologie entsprechende Leitlinien und Empfehlungen für die IT-Resilienz ausgearbeitet, die einige spezifische Instrumente (wie intelligente Stromzähler) berücksichtigen.

Schliesslich müssen auch die Kantone die Möglichkeit haben, in ihren Anforderungen weiter zu gehen als das Bundesgesetz. Dies ist ein Ausdruck des Subsidiaritätsprinzips.

Die Rolle des BACS für das Vorantreiben unseres Vorschlags

Obwohl die Kompetenzverteilung zwischen dem BACS und der Fachstelle des Bundes für Informationssicherheit unklar ist, muss das BACS seine Kompetenzen in Bezug auf die Cybersicherheit kritischer Infrastrukturen beibehalten. Da die Behörden und Organisationen des Bundes Teil der kritischen Infrastrukturen sind, bedauern wir die Entscheidung, in den kommenden Jahren zahlreiche Kompetenzen bezüglich ihrer Cybersicherheit an die Fachstelle des Bundes für Informationssicherheit zu übertragen.

Das zukünftige Bundesamt sollte die Umsetzung der Minimalanforderungen koordinieren. Darüber hinaus sollte es in der Lage sein, alle kritischen Infrastrukturen zu unterstützen, zum Beispiel bei der Verfügung von technischen Informationen zu aktuellen Cyberbedrohungen oder Empfehlungen für präventive und reaktive Massnahmen gegen Cybervorfälle (Art. 74 ISG).

Das Bundesamt spielt eine Schlüsselrolle bei der Umsetzung und Überwachung der Umsetzung unserer Empfehlung. Im Zusammenhang mit der Meldepflicht von Cyberangriffen verfügt es bereits über Aufsichtskompetenzen. Es wäre sinnvoll, die Rolle des BACS zu stärken und ihm die Möglichkeit zu geben, verschiedene Überwachungs- und Durchsetzungsmassnahmen durchzuführen (z. B. Inspektionen oder Audits, Zugang zu Informationen oder die Ausstellung von Warnungen). Dies erfordert auch die Bereitstellung von Ressourcen (Personal, Finanzen usw.) auf Bundesebene, um das Gesetz umzusetzen.

Schliesslich sind auch Sanktionen im ISG für den Fall der Nichteinhaltung notwendig. Diese sollen Organisationen davon abhalten, die Mindestanforderungen nicht einzuhalten, wie es bei Verstössen gegen die Meldepflicht für Cyberangriffe geplant ist. Es ist möglich, einen mehrstufigen Prozess beizubehalten (mit einer Information und Warnung durch das BACS, bevor eine Entscheidung getroffen und ein tatsächliches Sanktionsverfahren eingeleitet wird, ähnlich dem System in Art. 74 g let. h ISG2). Dieser Mechanismus würde es ermöglichen, das Vertrauen der kritischen Infrastrukturen gegenüber dem BACS zu erhalten.

Auch wenn wir davon überzeugt sind, dass die Regulierung der Cybersicherheit eine sehr positive Auswirkung auf die Reduktion der Cyberrisken in der Schweiz haben wird, muss an dieser Stelle zum Abschluss festgehalten werden, dass dies kein Ersatz für die Eigenverantwortung der einzelnen Organisationen ist. Cybersicherheit ist immer eine gemeinschaftliche Anstrengung aller involvierter Akteure.

Unsere Empfehlung in drei Schritten

1. **Eine Neudefinition des Begriffs «kritische Infrastruktur» und eine Erweiterung des Anwendungsbereichs der Mindestanforderungen an die Cybersicherheit im ISG.**
2. **Eine Verschärfung der bestehenden Mindestanforderungen.**
3. **Die Einführung zusätzlicher gesetzlicher Anforderungen an IT-Dienste, insbesondere an digitale Sicherheitsdienste.**

Impressum

Redaktion
Pauline Meyer, Sylvain Métille

Forschungsteam
Markus Christen, Melanie Knieps, *Digital Society Initiative, Universität Zürich.*
David-Olivier Jaquet-Chiffelle, Sylvain Métille, Pauline Meyer, Delphine Sarrasin, *Faculté de droit, des sciences criminelles, et d'administration publique, Université de Lausanne*.
Reto Inversini, *Nationales Zentrum für Cybersicherheit.*

Design
Rosa Guggenheim, guggenheim.li

Kontakt für Fragen
christen@ethik.uzh.ch, pauline.meyer@unil.ch

Dieses Dokument ist in Deutsch und Französisch erhältlich.