Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK

21. September 2023

# Erläuternder Bericht zum Vorentwurf zur Revision vom Mai 2024 der Stromversorgungsverordnung (Schutz vor Cyberbedrohungen)

# 1. Ausgangslage

Informations- und Kommunikationstechnologien (IKT) unterstützen die Entwicklung einer flexiblen und effizienten Energieversorgung. Zu diesem Zweck werden sie zunehmend zur Überwachung und Steuerung von Versorgungsnetzen und bei der Energieerzeugung eingesetzt. Sie tragen zwar zur Optimierung bei, vergrössern aber auch die Angriffsfläche für Cyberkriminelle und stellen somit neue Risiken dar.

Die Sicherheit der Energieversorgung ist von strategischer Bedeutung. Ihr sicherer Betrieb garantiert den Schutz wichtiger Rechtsgüter. Unser sozioökonomisches System ist so stark von der Energie abhängig, dass ein schwerwiegender Ausfall der Erzeugung oder der Verteilung gravierende Folgen hätte. Die Bedrohung eines Cyberangriffs auf die Energienetze hat deutlich zugenommen und ist heute höchst realistisch.

Die Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022 (SKI)[1] und die neue Nationale Cyberstrategie (NCS)[2] sehen geeignete Massnahmen vor, um die allgemeine Widerstandsfähigkeit kritischer Infrastrukturen zu erhöhen. Die NCS unterstützt dazu die Umsetzung des vom Bundesamt für wirtschaftliche Landesversorgung (BWL) ausgearbeiteten Minimalstandards zur Verbesserung der IKT-Resilienz[3] (IKT-Minimalstandard) und erwägt eine Verpflichtung, wo dies notwendig ist[4]. Die Anwendung dieses Dokuments ist freiwillig und die darin festgehaltenen Massnahmen werden daher in der Schweizer Energiewirtschaft bisher nicht systematisch umgesetzt.

Aufgrund der zunehmenden Bedrohungen und der Kritikalität ist es zwingend notwendig, ein hohes Cybersicherheitsniveau garantieren zu können. Obwohl die von den Akteuren der Branche bisher unternommenen Anstrengungen begrüsst werden, sind sie angesichts der Professionalisierung und Organisation krimineller Gruppen insgesamt noch zu wenig weitgehend und zudem nicht genügend verbreitet. Der 2021 veröffentlichte Grundlagenbericht des Bundesamts für Energie (BFE) zur Cybersicherheit[5] zeigt auf, dass in der Stromversorgung zurzeit kein genügend hoher Schutz besteht und daher ein regulatives Eingreifen des Staates notwendig ist. Aktuelle Entwicklungen im Bereich der künstlichen Intelligenz (z. B. ChatGPT) werden die Arbeit der Cyberkriminellen zusätzlich erleichtern. Die Resilienz der Cybersicherheit im Stromsektor muss verbessert werden, um nicht nur den aktuellen, sondern auch den künftigen Herausforderungen gewachsen zu sein.

# 2. Grundzüge der Vorlage

Die Revision der Stromversorgungsverordnung vom 14. März 2008 (StromVV; SR 734.71) hat zum Ziel, den IKT-Minimalstandard für die wichtigsten Stromversorger für verbindlich zu erklären. Die damit verpflichteten Akteure haben bei der Umsetzung der im Standard vorgesehen Massnahmen ein gewisses Schutzniveau zu erreichen. Im Sinne der Verhältnismässigkeit werden mehrere Schutzniveaus (Schutzprofile) mit abgestuften Anforderungen vorgesehen.

## 2.1 IKT-Minimalstandard

Der IKT-Minimalstandard legt eine Reihe von Massnahmen fest und ist ein wichtiges Instrument, um den Schutz vor Cyberangriffen zu gewährleisten. Der Standard basiert auf dem US-amerikanischen NIST Cybersecurity Framework[6]. Er enthält 108 Massnahmen, die in 23 Kategorien unterteilt sind. Die

1 BBl 2018 503
2 www.ncsc.admin.ch > NCS Strategie > Nationale Cyberstrategie NCS
3 Bundesamt für wirtschaftliche Landesversorgung, «Minimalstandard zur Verbesserung der IKT-Resilienz», Bern, 2023
4 Massnahme 6, *Resilienz, Standardisierung und Regulierung*, NCS, S. 21-22
5 Bundesamt für Energie, «Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung», Bern, Juni 2021
6 www.nist.gov/cyberframework

organisatorische Maturität der Cybersicherheit in einem Unternehmen kann mit Hilfe dieser Struktur bewertet und verbessert werden.

Die grundlegenden Massnahmen des Standards sind im Wesentlichen unveränderlich, erfordern jedoch für ihre Umsetzung eine gewisse Flexibilität, Anpassung an unternehmensspezifische und neue Bedrohungen und Gefährdungen, technische Hilfsmittel und entsprechendes Fachwissen[7]. Es werden darin keine technischen Lösungen vorgeschrieben. Die Unternehmen werden diese selbständig zu erarbeiten haben. Sie können sich hierzu auch im Rahmen der bestehenden Verbandsstrukturen zusammenschliessen und einen entsprechenden branchenspezifischen Standard erarbeiten.

## 2.2 Schutzniveau (Schutzprofil)

Das Schutzniveau definiert die Anforderungen an das Mass der Umsetzung der im IKT-Minimalstandard festgehaltenen Massnahmen (Werte / Tier Level gemäss Kapitel 3 des IKT-Minimalstandards). Die höchsten Anforderungen enthält das Schutzniveau A, die Schutzniveaus B und C enthalten jeweils etwas geringere Anforderungen. Für die kleinsten Marktakteure werden mit dem Schutzniveau C nur Vorgaben für eine begrenzte Anzahl von Massnahmen vorgesehen. Massnahmen für die keine entsprechenden Werte festgelegt werden, müssen nicht zwingend umgesetzt werden und bleiben daher unverbindliche Empfehlungen. Die einzelnen Schutzniveaus finden sich im neuen Anhang 1*a*. Die darin festgehaltenen Werte wurden für jedes Schutzniveau auf der Grundlage der Kritikalität der Unternehmen und unter Berücksichtigung der zur Umsetzung erforderlichen Mittel festgelegt. Sie wurden in einer Arbeitsgruppe des Verband Schweizerischer Elektrizitätsunternehmen (VSE) unter Einbezug von Experten des BFE erarbeitet.

Um die verpflichteten Unternehmen einem Schutzniveau (A, B oder C) zuzuordnen, werden entsprechende Kriterien festgelegt. Sofern ein Unternehmen die Kriterien eines Schutzniveaus erfüllt, ist dieses für das Unternehmen massgebend. So gilt beispielsweise das Schutzniveau A für Netzbetreiber, die eine transportierten Elektrizität von mindestens 450 GWh/Jahr erreichen (Ziff. 1.1 Anhang 1*a*). Bei der Festlegung der Kriterien wurden die Analysen und Praktiken anderer Fachstellen berücksichtigt. So entspricht das Kriterium von 450 GWh/Jahr, mit dem Netzbetreiber dem Schutzniveau A zugeordnet werden, einem vom Bundesamt für Bevölkerungsschutz (BABS) für die kritischen Infrastruktur von nationaler Bedeutung festgelegten Wert. Das Kriterium von 112 GWh/Jahr für das Schutzniveau B der Netzbetreiber und Dienstleister entspricht im Wesentlichen dem annualisierten Wert, der gemäss VSE eine Krise kennzeichnet[8].

Für die Erzeuger und die Speicherbetreiber wurde eine Leistung von 800 MW für das Schutzniveau A und 100 MW für das Schutzniveau B gewählt. Letztere entspricht dem in der Energieverordnung[9] definierten Wert für Pumpspeicherkraftwerke von nationalem Interesse.

Erzeuger, Speicherbetreiber und Dienstleister der beiden Akteure werden unter einer Leistung von 100 MW nicht von der Pflicht zur Einhaltung des IKT-Minimalstandards erfasst. Ein Schutzprofil C ist für sie nicht vorgesehen. Soweit der Schwellenwert von 100 MW nicht erreicht wird, bleibt für sie der Standard lediglich eine Empfehlung. Dies zum einen, weil ihr Einfluss auf die Versorgungssicherheit weniger hoch ist als bei den direkt via Steuertechnologie auf das Netz zugreifenden Netzbetreibern und zum anderen auch, weil sie die Kosten der Cybersicherheit im Gegensatz zu den Netzbetreibern nicht in die Tarife einrechnen können.

---

7 Jedes Unternehmen kann durch eine Risikoanalyse selbst feststellen, ob die verpflichteten Minimalmassnahmen ausreichend oder zusätzliche Massnahmen erforderlich sind. Der Leitfaden Schutz kritischer Infrastrukturen (SKI), herausgegeben vom Bundesamt für Bevölkerungsschutz (BABS), kann die Unternehmen bei dieser Aufgabe unterstützen. Der Leitfaden ist abrufbar unter www.infraprotection.ch > Schutz kritischer Infrastrukturen > Leitfaden SKI.

8 Verband Schweizerischer Elektrizitätsunternehmen (VSE), «ICT Continuity», 2011

9 Artikel 8 Absatz 4 der Energieverordnung vom 1. November 2017 (EnV; SR 730.01)

Soweit externe Dienstleister, die im Auftrag eines Unternehmens die IKT-Systeme verwalten, dauerhaft Zugriff auf die Steuersysteme (operativen Leitsysteme) der Auftraggeber haben, müssen sie dieselben Vorgaben wie die Auftraggeber einhalten.

# 3. Finanzielle, personelle und weitere Auswirkungen auf Bund, Kantone und Gemeinden

Zur Umsetzung der angestrebten Änderungen fallen bei Bund, Kantonen und Gemeinden keine nennenswerten personellen oder finanziellen Kosten an. Der Revisionsentwurf zielt darauf ab, das Cybersicherheitsniveau des Stromsektors zu erhöhen. Das bietet mittel- und langfristig einen besseren Schutz vor Cyberbedrohungen, wovon letztlich Bund, Kantone und die Gemeinden profitieren. Ausfälle aufgrund von Cyberangriffen wären mit weitreichenden Kostenfolgen verbunden.

# 4. Auswirkungen auf Wirtschaft, Umwelt und Gesellschaft

Die wirtschaftlichen, ökologischen und sozialen Folgen eines Cyberangriffs können sehr schwerwiegend sein. So können die durch einen Ransomware-Angriff verursachten Kosten (Lösegeld, Datenverlust, Zeit für die Wiederherstellung des Betriebs usw.) die Kosten für die Sicherung der Infrastruktur eines Unternehmens übersteigen. Die durch ein entsprechendes Cyberschutzniveau vermiedenen Kosten und damit der Nutzen der angestrebten Revision sind also entsprechend hoch.

Da bereits nach bestehender Regelung entsprechende Vorkehrungen für einen sicheren Netzbetrieb zu treffen sind (Art. 8 Stromversorgungsgesetz vom 23. März 2007 [StromVG; SR 734.7] und Art. 5 StromVV), sollten sich keine nennenswerten Mehraufwände ergeben. Risikobewusste Unternehmen, die bereits Sicherheitsmassnahmen umgesetzt haben, werden nur geringe oder keine zusätzlichen Kosten zu tragen haben. Mit wesentlichen Auswirkungen haben nur Unternehmen zu rechnen, die entgegen den bestehenden Vorgaben in diesem Bereich bisher untätig waren.

Im Allgemeinen werden die Kosten der Cybersicherheit für ein Unternehmen auf ca. 6 bis 14 % der IT-Ausgaben oder ca. 0,3 bis 0,5 % des Jahresumsatzes geschätzt. Diese Kosten müssen jedoch in Beziehung zu den Kosten eines Cybervorfalls, beispielsweise einer Erpressung durch Hacker nach einem Ransomware-Angriff gesetzt werden, bei dem die durchschnittlichen Kosten für ein KMU auf 1,4 Millionen Franken[10] geschätzt werden und für grosse Unternehmen weitaus höher liegen.

# 5. Verhältnis zum europäischen Recht

Die Europäische Union ist bestrebt, die Cybersicherheit in ihrem gesamten Gebiet zu verbessern und die Resilienz ihrer kritischen Infrastrukturen zu erhöhen. In diesem Zusammenhang zu berücksichtigen ist insbesondere die sogenannte NIS-Richtlinie[11] respektive deren Nachfolgeregelung, die NIS-2-Richtlinie[12]. Die EU sieht darin namentlich vor, dass die Mitgliedstaaten Massnahmen zum Schutz bedeutender Energieunternehmen vorzusehen haben[13]. Die allgemeinen Sicherheitsanforderungen der

[10] Sophos, «The State of Ransomware 2021», abrufbar unter news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/

[11] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194 vom 19.7.2016, S. 1

[12] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333 vom 27.12.2022, S. 80

[13] Siehe insbesondere Artikel 21 Absatz 1 und Anhang I NIS-2-Richtlinie

EU sind gestiegen und sie ist bestrebt, diese weiter zu erhöhen. Dazu werden in der EU zurzeit sogenannte Network Codes on Cybersecurity erarbeitet, die Vorgaben für verschiedene Aspekte der Cybersicherheit im Elektrizitätsbereich enthalten sollen.

Die vorliegende Regelung verbessert die Cybersicherheit im Stromsektor und sieht hierzu die Erarbeitung entsprechender Schutzmassnahmen vor. Sie entspricht dem Bestreben der EU, die Cybersicherheit im Elektrizitätsbereich weiter zu verbessern.

# 6. Erläuterungen zu den einzelnen Bestimmungen

*Artikel 1 Absatz 2*

Gemäss Artikel 1 Absatz 2 StromVV untersteht das mit der Frequenz 16.7 Hz und auf der Spannungsebene 132 kV betriebene Übertragungsnetz der schweizerischen Eisenbahnen (Bahnstromnetz) dem StromVG, soweit dieses bezweckt, die Voraussetzungen für eine sichere Elektrizitätsversorgung zu schaffen. Die Regelung von Artikel 8*a* StromVG[14] dient einer sicheren Elektrizitätsversorgung und würde demnach auch für den Bahnstrombereich zur Anwendung kommen. Für die Bahnstrom-Telematikanwendungen existieren indes bereits spezialrechtliche Vorgaben zur Cybersicherheit, die vom Bundesamt für Verkehr (BAV) überwacht werden[15]. Zur Vermeidung doppelter Zuständigkeiten (BAV – Eidgenössische Elektrizitätskommission [ElCom]) gelten daher die Vorgaben von Artikel 8*a* StromVG sowie die entsprechenden Ausführungsbestimmungen von Artikel 5*a* StromVV für den Bahnstrombereich nicht.

*Artikel 5a*

*Absatz 1:* Die Bestimmung enthält einen direkt-statischen Verweis auf den IKT-Minimalstandard. Der Standard wird damit in der erwähnten Version (2023) für verbindlich erklärt und die darin festgehaltenen Empfehlungen sind von den adressierten Akteuren unter Berücksichtigung der im Anhang 1*a* definierten Schutzniveaus (vgl. unten) umzusetzen. Erzeuger und Speicherbetreiber (Bst. b) sowie deren Dienstleister (Bst. c Ziff. 2) sind dieser Pflicht nur unterstellt, wenn der Zugriff auf die definierte Leistung über ein einziges System erfolgen kann. Für die Berechnung der Summe der Leistung ist vor dem Hintergrund eines Cyberangriff die Einflussnahme des Akteurs über das Steuerungssystem (industrielles Kontrollsystem / operatives Leitsystem) massgebend. Sind mehrere Steuersysteme in der Weise verbunden, dass eine Kompromittierung des einen Systems auch das andere System kompromittieren kann, so gelten sie als ein einziges System im Sinne dieser Bestimmung. Nicht verpflichtet wäre beispielsweise ein Erzeuger, der mehrere Anlagen von jeweils unter 100 MW Leistung über verschiedene, nicht verbundene Steuerungssysteme betreibt. Die Kernkraftwerksbetreiber (Inhaber der Betriebsbewilligung für ein Kernkraftwerk) werden gestützt auf Artikel 8*a* Absatz 2 StromVG vom Geltungsbereich der neuen Bestimmung ausgenommen, da für sie bereits entsprechende Vorgaben bestehen, die vom Eidgenössischen Nuklearsicherheitsinspektorat (ENSI) überwacht werden[16]. Der Fernzugriff eines Dienstleisters (Bst. c) ist dauerhaft, sofern dieser ihm im Rahmen eines Dauerschuldverhältnisses eingeräumt wurde, ohne dass die Auftraggeberin ihm jeweils ad hoc entsprechende Zugriffrechte erteilen muss.

*Absatz 2:* Die Bestimmung stellt klar, dass die im IKT-Minimalstandard erwähnten Regelwerke (Referenzen) nicht verbindlich sind.

[14] noch nicht in Kraft; vgl. Botschaft vom 2. Dezember 2022 zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), 22.073, BBl 2023 84

[15] AB-EBV zu Artikel 42, AB 42.2; Ausführungsbestimmungen zur Eisenbahnverordnung (AB-EBV; SR 742.141.11); zurzeit in Revision

[16] Artikel 5 und 6 der Verordnung des UVEK über die Gefährdungsannahmen und Sicherungsmassnahmen für Kernanlagen und Kernmaterialien (SR 732.112.1)

*Absatz 3:* Die ElCom überwacht aufgrund ihrer subsidiären Generalkompetenz (Art. 22 Abs. 1 StromVG) die Einhaltung von Artikel 8*a* StromVG und 5*a* StromVV.

*Anhang 1a:* Die Schutzniveaus (Schutzprofile) definieren die Anforderungen an den Umsetzungsgrad der im IKT-Minimalstandard definierten Massnahmen. Die höchsten Anforderungen enthält das Schutzniveau A für die für die Stromversorgung wichtigsten Unternehmen. Weniger hohe Anforderungen enthält das Schutzniveaus B für mittelgrosse und das Schutzniveau C für kleinere Akteure. Die Anforderungen werden entsprechend dem in Kapitel 3 des IKT-Minimalstandards festgelegten Prüfverfahren mittels sogenannten Werten (Tier Level) definiert. Diese reichen von «teilweise umgesetzt» (Wert 1) bis «dynamisch umgesetzt» (Wert 4). Als transportiere Elektrizität der Netzbetreiber (Ziff. 1.1 und 1.2) gilt die gesamte über ihr Netz geleitete Elektrizität (Verteilung zu den Endverbrauchern oder Weiterleitung zu anderen Netzen). Bei den Dienstleistern wird zur Bestimmung des massgebenden Schutzniveaus die Summe der transportierten Elektrizität (Netzbetreiber) beziehungsweise der installierten Leistung (Erzeuger und Speicherbetreiber) aller ihrer Auftraggeber berücksichtigt. Wenn ein Dienstleister über ein einziges System (vgl. oben zu Art. 5*a* Abs. 1) beispielsweise Zugriff hat auf die Steuersysteme von zehn Netzbetreibern mit einer transportierten Elektrizität von jeweils 13 GWh/Jahr, ergibt dies eine Summe transportierter Elektrizität von 130 GWh/Jahr. Der Dienstleister hat demnach die Werte des Schutzniveaus B zu berücksichtigen, während für jeden Netzbetreiber einzeln das Schutzniveau C massgebend wäre. Das Schutzniveau C für die kleineren Marktakteure enthält nur für rund 40 der insgesamt 108 Massnahmen des IKT-Minimalstandards verbindliche Vorgaben. Im Sinne der Verhältnismässigkeit sind damit nur die als prioritär eingestuften Massnahmen zu ergreifen. Sofern ein Akteur die Kriterien mehrerer Schutzniveaus erfüllt, ist das jeweils höchste Schutzniveau massgebend. Für die Überprüfung der Werte nach Anhang 1*a* stellt das BWL ein Formular auf seiner Webseite zur Verfügung[17].

[17] IKT-Minimalstandard Assessment Tool, abrufbar unter www.bwl.admin.ch > Themen > IKT > IKT-Minimalstandard