Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK

April 2023

Erläuternder Bericht zur Revision vom November 2023 der Rohrleitungssicherheitsverordnung

Inhaltsverzeichnis

1. Ausgangslage

Die Informations- und Kommunikationstechnologien (IKT) unterstützen die Entwicklung einer flexiblen und effizienten Energieversorgung. Dazu werden sie zunehmend für die Überwachung und Steuerung in Energieversorgungsnetzen genutzt. Zwar tragen sie dadurch zu Optimierungen bei, vergrössern aber auch die Angriffsfläche für Cyberkriminelle und stellen somit neue Risikoquellen dar.

Die Sicherheit der Energieversorgung ist von strategischer Bedeutung. Ihr sicherer Betrieb gewährleistet den Schutz wichtiger Rechtsgüter. Die Abhängigkeit unseres sozioökonomischen Systems von Energiequellen ist so gross, dass ein schwerwiegender Ausfall verheerende Folgen hätte. Die Bedrohung der Energienetze durch einen Cyberangriff ist heute sehr realistisch.

Die Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) 2018-2022[1] und die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022[2] halten entsprechende Massnahmen fest, um die allgemeine Widerstandsfähigkeit kritischer Infrastrukturen zu erhöhen. Die NCS[3] sieht dazu die Erarbeitung und Einführung von freiwilligen Mindeststandards der IKT-Sicherheit vor, was mit dem sogenannten IKT-Minimalstandard[4] entsprechend umgesetzt worden ist. Dieser Standard legt eine Reihe von Massnahmen fest und stellt ein wichtiges Hilfsmittel zur Sicherstellung des Schutzes gegen Cyberangriffe dar. Gestützt darauf hat die Branche Empfehlungen[5] ausgearbeitet, die erstmalig die notwendigen Grundlagen für die Cybersicherheit im Gasversorgungssystem geschaffen haben. Diese sogenannten Branchenstandards sind indes grundsätzlich freiwillig und werden noch nicht systematisch angewendet. Aufgrund der steigenden Bedrohungslage[6] ist es daher zwingend notwendig, mittelfristig solche Empfehlungen für diejenigen Unternehmen verbindlich zu erklären, deren Ausfall die schwerwiegendsten Folgen hätte. Damit die Empfehlungen für verbindlich erklärt werden können, müssen sie präzise und klar genug formuliert sein. Hierfür bedarf es einer zielgerichteten und raschen Überarbeitung der bestehenden Grundlagen sowie klaren Verantwortungen.

2. Grundzüge der Vorlage

Schon heute sieht Artikel 39 Absatz 3 der Rohrleitungssicherheitsverordnung vom 4. Juni 2021 (RLSV; SR 746.12) vor, dass die Betreiber ihre Einrichtungen vor störender äusserer Beeinflussung – und damit auch vor Cyberbedrohungen – zu schützen haben. Mit dem vorliegend neu eingeführten Artikel 39*a* wird die Pflicht zum Schutz vor Cyberbedrohungen einer spezifischen Regelung zugeführt und ein entsprechendes Verfahren zur Erarbeitung der dazu notwendigen Massnahmen festgelegt. Die Vorgabe adressiert aufgrund der technischen Vernetzung der IKT-Systeme und der damit verbundenen Risiken alle Betreiber, das heisst auch solche von Infrastrukturen mit einem Druck von 5 bar oder weniger (Art. 1 Abs. 2).

Der Bundesrat klärt damit die Verantwortung zum Schutz vor Cyberbedrohungen. Im Hinblick auf einen für die Zukunft angestrebten direkt-verbindlichen Verweis auf die Branchenstandards, ist es notwendig, diese zielgerichtet und unter Einbezug des Bundesamtes für Energie (BFE) zu überarbeiten respektive neu auszuarbeiten. Die vorliegende Regelung überträgt diese Aufgabe den Betreibern. Die dabei zu erarbeitenden Vorgaben sollten auf dem IKT-Minimalstandard des Bundesamts für wirtschaftliche Landesversorgung (BWL) sowie den bestehenden Branchenrichtlinien fussen. Sie sollten

[1] BBl 2018 503
[2] https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf
[3] Massnahme 8, Standardisierung und Regulierung, NCS 2018-2022, S.11
[4] Bundesamt für wirtschaftliche Landesversorgung BWL; «Minimalstandard zur Verbesserung der IKT-Resilienz», Bern, 2018 (zurzeit in Überarbeitung)
[5] G1008 Empfehlung, Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Gasversorgung, Ausgabe Dezember 2020
[6] NCS 2018-2022, S. 2

die betrieblichen und technischen Anforderungen präzisieren und dabei nach aktuellem Kenntnisstand folgende Rahmenbedingungen berücksichtigen:

1. Festlegung von unterschiedlichen Schutzprofilen. Jedes Schutzprofil umfasst technische und organisatorische Massnahmen auf einem unterschiedlichen Schutzniveau (bspw. Schutzprofil A für hohe Anforderungen, Schutzprofil B für mittlere Anforderungen und Schutzprofil C für niedrige Anforderungen).
2. Kriterien für die Zuordnung eines Betreibers zum entsprechenden Schutzprofil. Oft werden diese Kriterien, welche es erlauben die Betreiber entsprechend ihrer Kritikalität zu gruppieren, als «Unternehmensprofile» bezeichnet.
3. Präzisierung einzelner Anforderungen aus den bestehenden Standards. Eine mit der Branche durchgeführte Analyse hat gezeigt, dass einige der in dem IKT-Minimalstandard beziehungsweise in der Branchenrichtlinie aufgeführten Anforderungen präzisiert werden müssen.

Die Branche muss bei der Erarbeitung der vorgenannten Punkte das BFE als Aufsichtsbehörde beziehungsweise Oberaufsichtsbehörde für Rohrleitungsanlagen eng einbeziehen. Das BFE stellt die Koordination mit den relevanten Stellen der zentralen Bundesverwaltung (BWL, Bundesamt für Bevölkerungsschutz, Nationales Zentrum für Cybersicherheit [NCSC]) und dem Eidgenössischen Rohrleitungsinspektorat sicher.

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. Die vorliegende Anpassung führt nur zu einer moderaten Erweiterung des Pflichtenhefts des BFE, welche mit den bestehenden personellen und finanziellen Ressourcen abgedeckt werden kann.

Der Revisionsentwurf zielt darauf ab, das Cybersicherheitsniveau der Rohrleitungsanlagen 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 für das Land und die Gesellschaft sehr schwerwiegend sein. Ein Cyberangriff kann gravierende Konsequenzen haben, wie der Vorfall der Colonial Pipeline[7] in den USA zeigte. 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.

Die Umsetzung von Cybermassnahmen sind für die Unternehmen mit gewissen personellen und finanziellen Kosten verbunden. Da bereits nach bestehender Regelung entsprechende Vorkehrungen zu treffen waren, sollten sich indes keine nennenswerten Mehraufwände ergeben. Mit wesentlichen Auswirkungen haben nur Unternehmen zu rechnen, die entgegen den bestehenden Vorgaben in diesem Bereich bisher untätig waren. Risikobewusste Unternehmen, die angesichts der aktuellen Bedrohungen bereits Sicherheitsmassnahmen entlang der Branchenrichtlinie implementiert haben, werden kaum oder keine Mehrkosten zu tragen haben.

[7] https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

5. Verhältnis zum europäischen Recht

Die EU 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[8] respektive deren Nachfolgeregelung, die NIS-2-Richtlinie[9]. Die EU sieht darin namentlich vor, dass die Mitgliedstaaten Massnahmen zum Schutz bedeutender Energieunternehmen vorzusehen haben[10]. Die allgemeinen Sicherheitsanforderungen sind mit der NIS-2-Richtlinie gestiegen.

Die vorliegende Regelung verbessert die Cybersicherheit im Sektor der rohrleitungsgebundenen Energien und sieht hierzu die Erarbeitung entsprechender Schutzmassnahmen vor. Sie steht damit im Einklang mit den erwähnten Vorgaben der EU. Die bisherigen Arbeiten zu den Branchenstandards orientieren sich an internationalen Standards.

6. Erläuterungen zu den einzelnen Bestimmungen

Art. 39a Schutz vor Cyberbedrohungen

Absatz 1: Die von den Betreibern zu treffenden Massnahmen sollen Funktionsstörungen der entsprechenden Anlagen verhindern oder gegebenenfalls möglichst rasch beheben. Die Massnahmen sind sowohl organisatorischer (bspw. Inventarisierungsprozesse, Regelung von Zuständigkeiten, Sensibilisierungen) wie auch technischer Natur (bspw. Backups, Einsatz von Schutztechnologie).

Absatz 2 beauftragt die Betreiber, Richtlinien mit Massnahmen zum Schutz vor Cyberbedrohungen zu erarbeiten. Die Betreiber können sich hierzu im Rahmen der bestehenden Verbandsstrukturen (SVGW, VSG) entsprechend organisieren. Die bisherigen Arbeiten, die sich auf den IKT-Minimalstandard des BWL stützen, sollen in diesem Rahmen fortgeführt und präzisiert werden. Mit der vorgegebenen Konsultation wird die Einbindung aller interessierten Akteure gewährleistet. Neben den in der Bestimmung erwähnten Stellen ist insbesondere an das NCSC, das BWL und die Verbraucher zu denken. Die Durchführung der Konsultation ist in der Verantwortung der Betreiber.

Absatz 3: Die Vorgabe, wonach die Richtlinien über eine frei zugängliche Adresse im Internet zu veröffentlichen sind soll sicherstellen, dass der der Zugang zum entsprechenden Dokument nicht durch Logins oder dergleichen erschwert wird. Nach der Fertigstellung und der Publikation der Richtlinien durch die Betreiber wird das UVEK prüfen, ob sich diese dazu eignen, mit einem direkten Verweis in das Verordnungsrecht überführt zu werden (vgl. Art. 3 Abs. 2 und 3 RLSV). Die Betreiber haben insofern einen Anreiz zur Ausarbeitung einer möglichst sachgerechten Lösung (sog. gesteuerte Selbstregulierung).

[8] 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. 1–30
[9] 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; noch nicht in Kraft)
[10] Siehe insbesondere Artikel 21 Absatz 1 und Anhang I NIS-2-Richtlinie.