Weisung 1/2024

# Aufsicht Cybersicherheit der ElCom

8. Februar 2024

## 1 Ausgangslage

Gemäss Artikel 8*a* des revidierten Bundesgesetzes über die Stromversorgung vom 23. März 2007 (StromVG; SR 734.7) und Artikel 5*a* des Entwurfs zur Revision des Stromversorgungsverordnung vom 14. März 2008 (StromVV; SR 734.71), welche im Juli 2024 in Kraft treten, treffen Netzbetreiber, Erzeuger, Speicherbetreiber und Dienstleister (nachfolgend «Unternehmen») Massnahmen für einen angemessenen Schutz ihrer Anlagen vor Cyberbedrohungen. Für den sicheren und stabilen Systembetrieb des Schweizer Stromnetzes bedeutet dies, dass die Information Technology[1] (IT) und insbesondere die Operational Technology[2] (OT) gegen Cyberbedrohungen zu sichern sind.

Gemäss Artikel 22 Absatz 1 StromVG überwacht die ElCom die Einhaltung des StromVG und somit auch den Stand betreffend Massnahmen zum Schutz vor Cyberbedrohungen. Primärer Fokus der ElCom ist dabei der sichere und stabile Systembetrieb des Schweizer Stromnetzes. Basis der Aufsicht der ElCom bildet das NIST Cybersecurity Framework. Dies wird auch im IKT-Minimalstandard des Bundesamts für wirtschaftliche Landesversorgung (BWL), den Branchendokumenten des Verbands Schweizerischer Elektrizitätsunternehmen (VSE) sowie in den zukünftigen rechtlichen Vorgaben verwendet.

Damit die ElCom ihre Aufsichtstätigkeit ausüben kann, sind die Unternehmen gemäss Artikel 25 Absatz 1 StromVG verpflichtet, der ElCom die für den Vollzug des StromVG erforderlichen Auskünfte zu erteilen und die notwendigen Unterlagen zur Verfügung zu stellen.

Aufgrund des bevorstehenden Inkrafttretens des revidierten StromVG und der revidierten StromVV im Juli 2024 mit entsprechenden Vorgaben zum Schutz vor Cyberbedrohungen hat die ElCom ihr Konzept

[1] Information Technology meint dabei Technologien zur Datenverarbeitung, welche nicht direkt mit der Bereitstellung von Elektrizität zu tun haben (z.B. Kundendatenmanagement, Personaldatenmanagement, Büroanwendungen)

[2] Operational Technology meint dabei Technologien, welche direkt für die Bereitstellung oder Lieferung von Elektrizität notwendig sind (z.B. SCADA, PIA, Remote Access auf Installationen in Unterwerken, Rundsteuerung, Energiedatenmanagement (EDM), Smart Meter, intelligente Steuer- und Regelsysteme).

Eidgenössische Elektrizitätskommission ElCom
Christoffelgasse 5, 3003 Bern
Tel. +41 58 462 58 33, Fax +41 58 462 02 22
info@elcom.admin.ch
www.elcom.admin.ch

zur Aufsicht überarbeitet. Die vorliegende Weisung soll die zentralen Eckpunkte der regulatorischen Umsetzung dieser Aufsicht präzisieren. Sollten sich die Grundlagen, welche bei der Erarbeitung dieser Weisung Gültigkeit hatten, wesentlich ändern, behält sich die ElCom vor, diese Weisung anzupassen.

Mit dem geplanten Inkrafttreten der revidierten StromVV im Juli 2024 gelten für Netzbetreiber, Erzeuger, Speicherbetreiber und Dienstleister Minimalanforderungen im Bereich Cybersicherheit. In der revidierten StromVV werden die Minimalanforderungen entlang der fünf NIST-Kategorien «Identify, Protect, Detect, Respond und Recover» definiert. Diese gelten als Fundament für eine flächendeckende Steigerung der Resilienz der Schweizer Stromversorgung gegenüber Cyberbedrohungen.

Die Minimalanforderungen unterscheiden sich je nach Grösse und Art des Unternehmens und reichen je nach Risikoexposition eines Unternehmens für einen sicheren und stabilen Betrieb nicht aus. In jedem Fall bleiben die Unternehmen immer in der Verantwortung für den angemessenen Schutz ihrer Anlagen und Systemen vor Cyberbedrohungen. Die Minimalanforderungen der revidierten StromVV sind ab Inkrafttreten ohne Übergangsfrist verbindlich. Es liegt jedoch in der Aufsichtskompetenz der ElCom, die Frist und den Prozess hinsichtlich der Überprüfung der Erreichbarkeit der Minimalanforderungen zu regeln.

Für Netzbetreiber sind die Kosten für die Umsetzung von Cybersicherheits-Massnahmen anrechenbare Netzkosten, sofern sie die Anforderungen zur Anrechenbarkeit nach Artikel 15 Absatz 1 StromVG erfüllen. In der Mitteilung vom 28. September 2022 hat die ElCom die Anrechenbarkeit von Massnahmen zur Cybersicherheit präzisiert.

## 2 Aufsicht

Die ElCom verfolgt bei der Aufsicht einen risikobasierten Ansatz bezüglich des sicheren Systembetriebs des Schweizer Stromnetzes. Ziel der Aufsicht ist die Erhöhung der Resilienz gegenüber Cyberbedrohungen. Somit werden Unternehmen je nach Relevanz und Risikosituation für den sicheren und stabilen Systembetrieb des Schweizer Stromnetzes in unterschiedlicher Tiefe überwacht. Die Aufsichtsinstrumente sollen der ElCom eine Beurteilung ermöglichen, ob die getroffen Massnahmen den Risikoüberlegungen des Unternehmens entsprechen und die rechtlichen Vorgaben eingehalten sind. Dies bedeutet auch, dass die ElCom aufgrund ihrer Regulierungstätigkeit Empfehlungen abgeben und / oder Massnahmen anordnen kann. Zur Durchsetzung von Massnahmen stehen der ElCom die üblichen Rechtsmittel zur Verfügung. Aktuell sieht die ElCom vor, drei Aufsichtsinstrumente ergänzend einzusetzen und zu kombinieren.

### 2.1 Umfragen

Nach Inkrafttreten der revidierten StromVV haben die Unternehmen bestimmte Minimalanforderungen zu erfüllen. Die ElCom wird diese in einer ersten Phase über eine Selbsteinschätzung im Rahmen einer Umfrage auf Basis des BWL-Assessment-Tools erheben. Die eingereichten Selbsteinschätzungen müssen durch ein Schreiben der jeweiligen Geschäftsleitung bestätigt werden. Diese Umfrage wird jährlich bei allen gemäss revidierter StromVV betroffenen Unternehmen durchgeführt. Diese Umfrage erlaubt es der ElCom, einerseits eine Übersicht über das Erreichen der rechtlichen Vorgaben zu erstellen und anderseits Informationen über den Stand der Cybersicherheits-Massnahmen einzuholen und auszuwerten.

### 2.2 Sensibilisierungsgespräche

Sensibilisierungsgespräche werden in erster Linie mit Unternehmen mit besonderer Relevanz für den sicheren und stabilen Systembetrieb des Schweizer Stromnetzes geführt. Ergänzend sind Sensibilisierungsgespräche auch aufgrund auffälliger Antworten in den Umfragen oder einer zufälligen Stichprobe möglich. Ziel dieser Gespräche ist es, konkrete Informationen zur Umsetzung der Cybersicherheits-Massnahmen zu gewinnen und dadurch die Ergebnisse der Umfrage qualitativ zu ergänzen. Die Sensibilisierungsgespräche finden regelmässig vor Ort bei den relevanten Unternehmen statt. Die Erkennt-

nisse aus den Gesprächen bilden eine Grundlage für die Einschätzung der Cybersicherheit beim Unternehmen sowie der Ableitung allfälliger Empfehlungen für Massnahmen. Deren Umsetzung kann in den nachfolgenden Sensibilisierungsgesprächen geprüft werden.

### 2.3 Audits

Als drittes Aufsichtsinstrument kann die ElCom individuelle Audits durchführen. Diese sollen bestimmte technische Aspekte aufgrund von Auffälligkeiten bei der Umfrage oder den Sensibilisierungsgesprächen vertiefen. Ebenso können Audits aufgrund von externen Hinweisen oder einer zufälligen Stichprobe durchgeführt werden. Je nach Ziel und Zweck können diese Audits durch die ElCom oder durch einen externen Auditor durchgeführt werden.

## 3 Übergang Minimalanforderungen StromVV

Die revidierte StromVV sieht zur Erreichung der geforderten minimalen Zielwerte keine Übergangsfrist vor. Damit die Selbsteinschätzungen aus der Umfrage bei den Unternehmen den Ist-Zustand möglichst gut abbilden, erlaubt die ElCom eine Übergangsfrist zum Nachweis der Erreichung der geforderten Zielwerte von maximal 24 Monaten nach Inkrafttreten der revidierten StromVV.

Für die Kategorien, in denen die Zielwerte nicht erreicht wurden, ist ein von der Geschäftsleitung bestätigter Massnahmen- und Umsetzungsplan mit konkreten verbindlichen Umsetzungszielen einzureichen. Werden aus Sicht der ElCom die darin vorgeschlagenen Massnahmen nicht zeitnah umgesetzt, sucht die ElCom das Gespräch mit den betroffenen Unternehmen. Liegen nachvollziehbare Gründe vor, dass die Zielwerte nicht innerhalb der Übergangsfrist erreicht werden konnten, kann die ElCom ausnahmsweise eine weitere Frist gewähren.

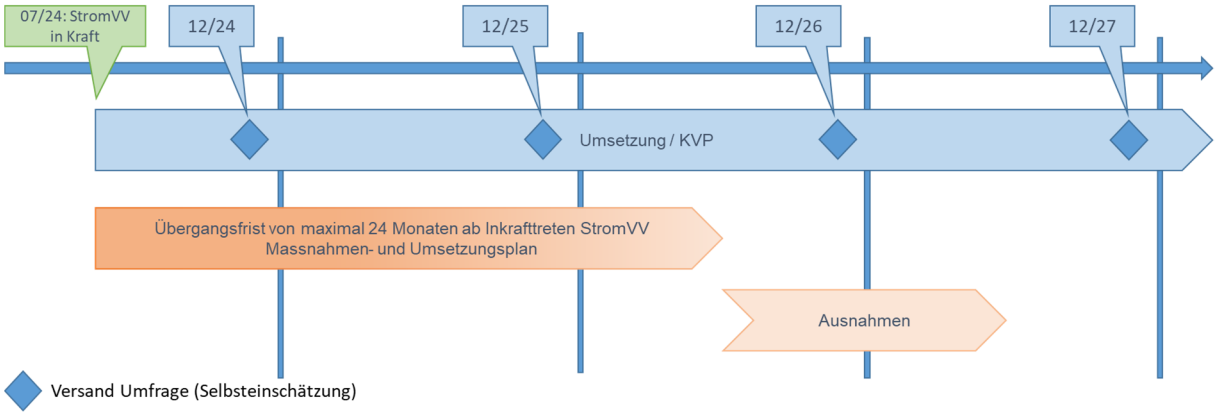


Abbildung: Ablaufschema Umsetzung Cybersicherheit-Minimalanforderungen