Swissgrid AG
Bleichemattstrasse 31
Postfach
5001 Aarau
Schweiz

T +41 58 580 21 11
info@swissgrid.ch
www.swissgrid.ch

Ihr Kontakt
Michael Rudolf
T direkt +41 58 580 35 15
michael.rudolf@swissgrid.ch

Per E-Mail an: ncsc@ncsc.admin.ch

13. September 2024

Stellungnahme Swissgrid: Vernehmlassung Cybersicherheitsverordnung (CSV)

Sehr geehrte Damen und Herren

Besten Dank für die Möglichkeit zur Stellungnahme zur im Betreff erwähnten Vernehmlassungsvorlage.

Als nationale Netzgesellschaft sorgt Swissgrid dauernd für einen diskriminierungsfreien, zuverlässigen und leistungsfähigen Betrieb des Übertragungsnetzes als wesentliche Grundlage für die sichere Versorgung der Schweiz (Art. 20 Stromversorgungsgesetz, StromVG).

Swissgrid hatte bereits im Rahmen der Vernehmlassung des Informationssicherheitsgesetzes von 2022 die Einführung einer Meldepflicht für Cyberangriffe begrüsst. Vorliegender Entwurf der Cybersicherheitsverordnung (CSV) ist unserer Ansicht nach eine gute Grundlage zur Präzisierung und Regelung dieser Meldepflicht. An folgenden Stellen sehen wir Ergänzungs- und Präzisierungsbedarf:

Art. 2 Nationale Cyberstrategie

Für Swissgrid ist nicht ersichtlich, weshalb in Art. 2 Abs. 2 CSV die nationale Cyberstrategie «nur» in Abstimmung mit den Kantonen festgelegt wird und nicht auch in Abstimmung mit weiteren bedeutenden Interessengruppen (vgl. Art. 4 Abs. 1 CSV) **inkl. Betreibern von kritischen Infrastrukturen.**

Art. 4 Zusammensetzung des StA NCS

Änderungsantrag:

[1] Der StA NCS setzt sich aus Vertreterinnen und Vertretern der Departemente, der Bundeskanzlei, der Kantone, der Wirtschaft, **der kritischen Infrastrukturen,** der Gesellschaft und der Hochschulen zusammen.

[3] Er ernennt aus dem Kreis der Vertreterinnen und Vertreter der Wirtschaft, **der kritischen Infrastrukturen,** der Gesellschaft und der Hochschulen die vorsitzende Person.

Begründung: Swissgrid beantragt eine explizite Nennung der Betreiber von kritischen Infrastrukturen in Art. 4 Abs. 1 CSV. Die Erläuterungen weisen auf Seite 6 darauf hin, «*dass sämtliche Vorgaben zur Cybersicherheit der Bundesverwaltung, die Zuständigkeiten und Aufgaben der Fachstelle des Bundes für Informationssicherheit und die sich daraus ergebenden Schnittstellen zu den Aufgaben des BACS in der ISV [und damit nicht in der CSV] geregelt werden*». **Die Betreiber von kritischen Infrastrukturen sind somit zentral Betroffene der CSV, weshalb sie auch explizit in Art. 4 CSV aufzunehmen sind**.

Art. 15 Übermittlung und Nutzung der Informationen

Für Swissgrid bestehen bei Art. 15 CSV folgende Fragen:

- Was sind die Folgen, wenn eine TLP-Klassifizierung nicht eingehalten wird?
- Welche TLP-Protokoll Vorgabe ist zu verwenden, sollte der Informationslieferant den Empfängerkreis nicht festlegen? Aus Sicht Swissgrid ist in diesem Fall (bis zur Klärung) «TLP amber strict» anzuwenden.

Wir beantragen entsprechende Ergänzungen der Verordnung oder der Erläuterungen.

Art. 16 Ausnahmen von der Meldepflicht

Art. 16 Abs. 1 Bst. b Ziffer 1 CSV verweist auf Art. 5a Abs. 1 und Anhang 1a der Stromversorgungsverordnung (StromVV) resp. die dortigen Minimalstandards. Die dortigen Bestimmungen regeln u.a. die Pflichten von «*Dienstleistern, die dauerhaft Anlagen von Netzbetreibern fernsteuern können*». Aus Sicht Swissgrid sind von der Meldepflicht auch **Dienstleister** zu erfassen**, welche intelligente Mess- und Steuersysteme steuern**, sofern sie den entsprechenden Grenzwert nach Anhang 1a StromVV erfüllen. Wir beantragen eine entsprechende Überprüfung und ggf. Anpassung der Vernehmlassungsvorlage.

Bei der Ausarbeitung der Minimalstandards gemäss StromVV ist zudem darauf zu achten, dass dies möglichst EU-kompatibel erfolgt.

Begründung: Gemäss Art. 31e StromVV sind bis 2027 80% aller Messeinrichtungen mit einem intelligenten Messsystem auszustatten. Intelligente Messsysteme müssen gemäss Art. 8a Abs. 1 Bst. a Ziffer 3 StromVV über eine bidirektionale Kommunikation verfügen. D.h. die Messsysteme können ein Signal empfangen und darauf bspw. eine Rundsteuerung oder Wärmepumpe ansteuern. Im Rahmen des Bundesgesetzes über eine sichere Stromversorgung mit

erneuerbaren Energien (sog. «Stromgesetz») ist weiter die Einführung einer zentralen Datenplattform (Datahub) vorgesehen. Dadurch und aufgrund weiterer Bestimmungen des Stromgesetzes dürften die Pflichten der Verteilnetzbetreiber hinsichtlich Datenerfassung und Datenaustausch erheblich zunehmen. Swissgrid vermutet, dass zunehmend mehr (kleine) Verteilnetzbetreiber Aufgaben im Zusammenhang mit intelligenten Mess- und Steuersystemen an Dienstleister auslagern und somit bei diesen bündeln werden.

Art. 19 Inhalt der Meldung

Änderungsantrag:

[1] Die Meldung muss folgende Informationen zum Cyberangriff enthalten:

d. Angriffsmethode; ~~und~~

e. **sofern bekannt,** Angaben zum Verursacher**; und**

f. Angegriffene Systeme.

Begründung: Eine Zuordnung eines Angriffs an einen Verursacher dürfte – gerade im Hinblick auf die Meldefrist von 24 Stunden – in vielen Fällen nur schwer (zuverlässig) durchführbar sein. Die Informationen sind somit «sofern bekannt» zu liefern. Zudem schlagen wir vor, dass auch Informationen zu den angegriffenen Systemen in die Meldung aufzunehmen sind. Diese Information dürfte insbesondere im Falle von weitverbreiteten Applikationen von Standardanbietern relevant sein.

Art. 21 Frist zur Erfassung der Meldung

Gemäss Erläuterungen stützt sich Art. 21 CSV auf Art. 74e ISG. Gemäss diesem hat die Meldung innert 24 Stunden nach der Entdeckung des Cyberangriffs zu erfolgen. Im Sinne der Verständlichkeit regen wir an, dass dies in Art. 19 CSV ergänzt wird oder ein direkter Verweis auf Art. 74e Abs. 1 ISG aufgenommen wird.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
Swissgrid AG

Roger Wirth
Head of Cyber Security

Michael Schmid
Head of Legal, Regulatory & Compliance