swissgrid

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

Nationales Zentrum für Cybersicherheit
Schwarztorstrasse 59
CH-3003 Bern

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

5. April 2022

Swissgrid Stellungnahme zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

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). Das Übertragungsnetz bzw. die Stromversorgung ist die kritischste Infrastruktur der Schweiz[1]. Gerne äussern wir uns zum Entwurf einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe.

Swissgrid begrüsst die Einführung einer Meldepflicht für Cyberangriffe nach Art. 74a des vorliegenden Entwurfs des Informationssicherheitsgesetzes (ISG). Die bisher auf Freiwilligkeit basierende Regelung in Art. 76 Abs. 3 ISG ist nicht ausreichend. Damit die Schweiz ihre kritischen Infrastrukturen vor Cyberangriffen schützen kann, müssen die dafür zuständigen Stellen beim Bund Kenntnis über Herkunft, Methodik und Ausmass von Cyberangriffen haben. Die vom Bund gesammelten resp. daraus gewonnen Erkenntnisse müssen wiederum mit Betreiberinnen kritischer Infrastrukturen geteilt werden können.

Bei den Bestimmungen des vorliegenden Entwurfs sehen wir an verschiedenen Stellen Präzisierungsbedarf. Zudem besteht unserer Ansicht nach Abstimmungsbedarf mit dem revidierten Datenschutzgesetz (revDSG). Dies betrifft u.a. die Meldepflicht im revDSG bei der Verletzung der Datensicherheit.

[1] Vgl. u.a. Bericht des Bundesamtes für Bevölkerungsschutz BABS (2020) «Katastrophen und Notlagen Schweiz 2020, Bericht zur nationalen Risikoanalyse»

Zu den Bestimmungen haben wir folgende Anmerkungen:

Art. 5 Begriffe

In diesem Gesetz bedeuten:

d. Cybervorfall: Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist;

e. Cyberangriff: Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde.

Bst. d: Mit der Formulierung «Beeinträchtigung der Nachvollziehbarkeit» unterscheidet sich das ISG von Datenschutzgesetzen, die vor allem die Vertraulichkeit, Integrität und Verfügbarkeit von Personendaten sicherstellen wollen. Will das ISG mit dieser Formulierung absichtlich zur Meldung einer weiteren Form der Beeinträchtigung anregen? Und wenn Ja, an welches Szenario ist bei einer Beeinträchtigung der Nachvollziehbarkeit einer Informations-Bearbeitung zu denken?

Bst. e: Für Swissgrid ist unklar, ob «Unbefugte» auch betriebsinterne Personen miteinschliesst, die absichtlich über ihre Kompetenzen hinaus eine Beeinträchtigung der «Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung» herbeiführen. Weiter ist für Swissgrid unklar, ob Bst. e nur «erfolgreich» durchgeführte Cyberangriffe oder auch versuchte Angriffe («near misses») erfasst. Die Unklarheit ergibt sich für Swissgrid einerseits aus dem Verweis auf Bst. d, wo schon die blosse Möglichkeit einer Beeinträchtigung erfasst ist und andererseits aus Art. 74d Abs. 1 – insbesondere aus Bst. a und c (Anzeichen einer potenziellen Gefährdung/Veränderung des Informationsbestands bereits Auslöser der Meldepflicht). Wir beantragen entsprechende Klarstellungen im Entwurf oder den Erläuterungen.

Art. 73b Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen

[2] *Das NCSC kann Informationen zu Cybervorfällen veröffentlichen oder an interessierte Behörden und Organisationen weiterleiten, sofern dies dazu dient, Cyberangriffe zu verhindern oder zu bekämpfen. Diese Informationen dürfen Personendaten und Daten juristischer Personen enthalten, sofern es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt und die betroffene Person einwilligt.*

Für Swissgrid ist unklar, wie der Einwilligungsprozess ablaufen soll bzw. wer für das Einholen der Einwilligung zuständig ist. Holt das NCSC die Einwilligung der betroffenen Person ein oder ist angedacht, dass dies das meldepflichtige Unternehmen tun muss? In letzterem Fall: Besteht für das meldepflichtige Unternehmen gar eine Mitwirkungspflicht, welche über die Auskunftspflicht in Art. 74g ISG hinausgeht? Swissgrid geht diesbezüglich davon aus, dass die Weitergabe von Personendaten, namentlich die Bekanntgabe von Kontaktdaten zur Ermöglichung der Einholung der Einwilligung durch das NCSC nicht durch die Art. 74e und 74g ISG abgedeckt ist. Die Weitergabe von Personendaten bedarf nach Ansicht von Swissgrid einer Grundlage im Gesetz (Mitwirkungspflicht).

Art. 73c Weiterleitung von Informationen

[4] *Informationen, die strafrechtlich geschützte Geheimnisse offenbaren, darf das NCSC nur nach den Vorgaben von Artikel 320 StGB weiterleiten.*

Swissgrid regt an, dass in den Erläuterungen namentlich erwähnt wird, durch welche Behörde sich das NCSC vom Geheimnisschutz entbinden lassen kann.

Art. 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen

Swissgrid begrüsst die in Art. 74 ISG verankerte Unterstützung von Betreiberinnen kritischer Infrastrukturen durch das NCSC. Der bereits heute etablierte Austausch zwischen Betreiberinnen kritischer Infrastrukturen und dem NCSC bzw. ehemals MELANI funktioniert gut. Eine Ausweitung dieses Modells dürfte indes eine Herausforderung darstellen. Swissgrid teilt die Ansicht der Erläuterungen (S. 27), dass dies seitens Bund zusätzliche Aufwände verursachen wird und deshalb beim Ausbau des NCSC zu berücksichtigen ist.

Art. 74a Meldepflicht

Sowohl der vorliegende Entwurf (Art. 74a) als auch das revDSG (Art. 24) verlangen, dass Meldungen an das NCSC resp. den EDÖB «so rasch als möglich» erfolgen. Unklar ist, in welchem Verhältnis diese Meldepflichten bzw. die beiden Gesetze zueinanderstehen. Haben die beiden Meldungen gleichzeitig zu erfolgen oder ist die Erwartung, dass die Meldung nach ISG zuerst erfolgt? Swissgrid geht von einem zeitlichen Vorrang der Meldung nach ISG aus, zumal die Formulierung von Art. 74e Abs. 2 ISG explizit die Möglichkeit eröffnet, nach einer ersten so rasch als möglich erfolgten Meldung, gewisse Informationen zu einem späteren Zeitpunkt nachzuliefern. Das revDSG sieht eine solche Möglichkeit nicht explizit vor. Die Frage stellt sich zudem, weil je nach Unternehmen unterschiedliche Funktionen (bzw. Personen) zuständig für die Entgegennahme von Informationen und das Absetzen der jeweiligen Meldungen sein können. Alleine dadurch können sich Verzögerungen der beiden Meldungen ergeben.

Gemäss Art. 74a ISG, ist es Aufgabe des NCSC, mögliche Betroffene zu warnen. Diesbezüglich weisen wir auf Fälle von unter falschem Namen (oder anderen Identifikationsmerkmalen wie bspw. Foto der Person) versendeten Phishing Mails hin. Es stellt sich die Frage, ob die Informierung der Person unter dessen Namen die Phishing Mail verschickt wurde, ebenfalls unter diese Bestimmung fällt, d.h. eine Informationspflicht des NCSC gegenüber dem/der (vermeintlichen) Absender/Absenderin besteht. Zu berücksichtigen ist dabei:

1) Zwischen der Person und dem NCSC besteht womöglich kein bisheriges Kontaktverhältnis. Hingegen kann ein solches mit dem meldepflichtigen Unternehmen bestehen. Ist vorgesehen, dass hier das meldepflichtige Unternehmen wiederum eine Mitwirkungspflicht bei der Informierung hat? Wenn Ja, sollte diese gesetzlich festgehalten werden.
2) Die Person kann zu den Geschädigten gehören oder aber die Täterschaft sein. Somit stellt sich die Frage, zu welchem Zeitpunkt die Informierung dieser Person zu erfolgen hat, bzw. welche allfälligen Abklärungen zuerst durchzuführen sind (um bspw. nicht eine Untersuchung oder Beweissicherung zu tangieren).

Art. 74c Ausnahmen von der Meldepflicht

Swissgrid kann den Grundgedanken der vorgesehenen Delegationsnorm an den Bundesrat bzgl. Ausnahmen von der Cybermeldepflicht nachvollziehen. Hinsichtlich Stromnetzbetreibern geben wir zu bedenken, dass ein Grossteil dieser nur wenige oder nur eine einzige Gemeinde versorgen. Die Stromversorgung bzw. das Stromnetz ist jedoch die kritischste Infrastruktur. Sie ist Grundlage für das Funktionieren zahlreicher anderer kritischer Infrastrukturen. Zudem geht Swissgrid von einem relativ hohen Standardisierungsgrad der eingesetzten Applikationen auf den unteren

Netzebenen aus. Ist ein Cyberangriff auf einen einzelnen Netzbetreiber erfolgreich, könnte der Angriff auch bei anderen Netzbetreibern erfolgreich sein. Eine Meldepflicht an den Bund mit anschliessender Weiterleitung von Erkenntnissen des Angriffs an weitere Netzbetreiber kann somit entscheidend zur Sicherheit des Gesamtsystems beitragen. Aus Sicht von Swissgrid, ist deshalb von einer allfälligen Anwendung der Ausnahmebestimmungen in Art. 74c ISG im Strombereich abzusehen.

Art. 74d Zu meldende Cyberangriffe

[1] *Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass:*

a. *die Funktionsfähigkeit der betroffenen kritischen Infrastruktur oder einer anderen kritischen Infrastruktur gefährdet ist;*

b. *ein fremder Staat ihn ausgeführt oder veranlasst hat;*

c. *er zu einem Abfluss oder zur Manipulation von Informationen geführt hat oder führen könnte*

Art. 74d stellt nach Ansicht von Swissgrid den «Kern» der Vorlage dar. Die Bestimmung erscheint jedoch noch nicht ausgereift und ist zu präzisieren.

Bei Bst. a stellt sich uns die Frage, ab wann eine Gefährdung der Funktionsfähigkeit der betroffenen kritischen Infrastruktur meldungsrelevant ist. Wie stark muss die Beeinträchtigung der Funktionsfähigkeit sein, damit eine Meldepflicht ausgelöst wird?

Auch im Hinblick auf die Gefährdung «einer anderen kritischen Infrastruktur» schafft die Bestimmung Unsicherheiten bzw. zu grossen Auslegungsspielraum. So stellt sich bspw. die Frage, wie ein Unternehmen erkennen kann, ob eine andere, ihm / ihr nicht im Detail bekannte kritische Infrastruktur derart von der Funktionsfähigkeit des Unternehmens abhängig ist, dass die kritische Infrastruktur bei einer Beeinträchtigung der Funktionsfähigkeit des Unternehmens gefährdet ist. Swissgrid beantragt weitere Präzisierungen bzgl. wann eine Meldepflicht einsetzt. In diesem Zusammenhang geben wir zu bedenken, dass detaillierte Konkretisierungen mit Blick auf die Vielfalt an kritischen Infrastrukturen subsidiär zu regeln sind. Swissgrid teilt diesbezüglich die Meinung in den Erläuterungen auf S. 26, dass sich der Bundesrat bei der Festlegung von Vorgaben an einschlägigen Fachnormen orientieren und diese auch für verbindlich erklären können soll.

Die in Bst. b. vorgesehene Einschätzung bzw. die Zuordnung eines Angriffs zu einem Staat durch den Betroffenen dürfte nur schwer bis gar nicht durchführbar sein. Dies vor allem nicht, wenn eine Meldung möglichst rasch erfolgen soll und damit zu einem Zeitpunkt, wo erst unvollständige Informationen zum Cyberangriff vorliegen. Weiter ist davon auszugehen, dass der Betroffene nicht in der Lage ist zu erkennen bzw. zu unterscheiden, ob ein Angriff staatlich geduldet, gefördert oder effektiv staatlich durchgeführt wurde und oder von der Täterschaft falsche Spuren gelegt wurden.

Aus Sicht Swissgrid ist die in Bst. c enthaltene Schwelle eher niedrig angesetzt und könnte damit bei fast jedem Cyberangriff erfüllt sein. Mit Blick auf das Stromnetz, sind aus Sicht von Swissgrid Cyberangriffe zu melden, wenn u.a. folgende Informationen oder Systeme betroffen bzw. beeinträchtigt sind:

- Besonders schützenswerte Personendaten;

- Informationen zu den kritischen Infrastrukturen und Systemen (inkl. Schnittstellen und Zugangsmöglichkeiten) der kritischen Infrastruktur Betreiberin;
- Daten des Stromnetzbetriebs; oder
- Infrastrukturen und Systeme, welche für die Erfüllung des Kernauftrags der kritischen Infrastruktur Betreiberin kritisch sind.

Art. 74e Inhalt der Meldung

[1] *Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.*

Zum Vergleich, Art. 24 revDSG

[2] *In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.*

Art. 74e Abs. 1 ISG enthält, anders als Art. 24 Abs. 2 revDSG, keine Pflicht, bereits ergriffene Massnahmen zu melden. Wurde darauf bewusst verzichtet?

Art. 74f Übermittlung der Meldung

[2] *Das System muss der Betreiberin einer kritischen Infrastruktur ermöglichen, die Meldung des Cyberangriffs oder seiner Auswirkungen gesamthaft oder in Teilen an weitere Stellen und Behörden zu übermitteln.*

Aus Sicht Swissgrid, hat das System insb. die Übermittlung der Meldung an den EDÖB zu ermöglichen. Zudem wäre es wünschenswert, wenn über das System auch die Informationen, welche dem EDÖB gemäss revDSG ergänzend zu liefern sind, übermittelt werden könnten.

Art. 74i Widerhandlungen gegen Verfügungen des NCSC

[1] *Mit Busse bis zu 100 000 Franken wird bestraft, wer einer vom NCSC unter Hinweis auf die Strafdrohung dieses Artikels erlassenen rechtskräftigen Verfügung oder dem Entscheid einer Rechtsmittelinstanz vorsätzlich nicht Folge leistet.*

[3] *Fällt eine Busse von höchstens 20 000 Franken in Betracht und würde die Ermittlung der nach Artikel 6 VStrR strafbaren Personen Untersuchungsmassnahmen bedingen, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären, so kann die Behörde von einer Verfolgung dieser Personen absehen und an ihrer Stelle den Geschäftsbetrieb zur Bezahlung der Busse verurteilen.*

Bei Art. 74i Abs. 1 ISG ist für Swissgrid unklar, ob unter «vorsätzlich» auch der Eventualvorsatz erfasst ist. Weiter stellt sich die Frage, wer die relevanten Personen sind, welche sanktioniert werden und ob diesbezüglich bewusst von den Verantwortlichkeiten im revDSG (Art. 63) abgewichen wird. Folgt man dem erläuternden Bericht des ISG, würde dies zudem bedeuten, dass unter Umständen eine andere Person (Person «in der Linie») für die Meldung verantwortlich wäre, aber eine Führungsperson («Leitungsebene von Unternehmen», Erläuterungen S. 22) zur Rechenschaft gezogen werden könnte. Soll eine Führungsperson sanktioniert werden, könnte diese Person durch Herausverlangen des Organigramms einfach bestimmt werden. Somit würde sich aber

Art. 74i Abs. 3 erübrigen, da keine «unverhältnismässigen Ermittlungen» erforderlich wären. Wir beantragen eine Prüfung und ggf. Überarbeitung dieser Bestimmung bzw. der Erläuterungen.

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

Freundliche Grüsse
Swissgrid AG

Konrad Zöschg
Head of Technology

Michael Schmid
Head of Legal, Regulatory & Compliance