Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Eidgenössisches Finanzdepartement
Nationales Zentrum für Cybersicherheit (NCSC)
3003 Bern

Elektronisch an: ncsc@gs-efd.admin.ch

28. März 2022

Markus Riner, Direktwahl +41 62 825 25 27, markus.riner@strom.ch

Stellungnahme zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Der Verband Schweizerischer Elektrizitätsunternehmen (VSE) dankt Ihnen für die Möglichkeit, sich zur Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe zu äussern. Er nimmt diese Gelegenheit gern wahr.

Der VSE vertritt als Dachverband die Interessen der schweizerischen Elektrizitätswirtschaft entlang der gesamten Wertschöpfungskette von der Produktion über den Handel bis zur Übertragung und Endverteilung von Strom. Eine sichere Stromversorgung ist für eine funktionierende Gesellschaft und Wirtschaft lebensnotwendig. Die Infrastrukturen der Strombranche gehören daher eindeutig mit zu den wichtigsten kritischen Versorgungsinfrastrukturen. Um diese möglichst effektiv vor den zunehmenden Cyberbedrohungen zu schützen, engagiert sich der VSE stark durch die Erarbeitung von Branchendokumenten und unterstützt die Branchenunternehmen in Belangen der Cybersicherheit. Der VSE hat sich ebenfalls aktiv und konstruktiv in die Grundlagenarbeiten für die vorliegende Gesetzesrevision des Informationssicherheitsgesetzes ISG eingebracht.

Betreffend die Änderungen des ISG unterstützt der VSE die vorgeschlagene gestärkte Positionierung des NCSC als zentrale Anlaufstelle des Bundes für die Wirtschaft, einschliesslich der Energiewirtschaft, bei Cyberfragen und als Unterstützerin bei der Bewältigung von Cyberangriffen. Dies entspricht den Erwartungen der Branche insbesondere zur gemeinsamen Verbesserung der Cybersicherheit im Rahmen der Meldepflicht.

Grundsätzlich erwartet der VSE vom NCSC im Ernstfall eines Cyberangriffs schnell verfügbare CERT Dienstleistungen zur Unterstützung bei der Analyse und präzisen Erfassung der Lage sowie bei der Initiierung der nötigen Schritte zur schnellen Abwehr und zur Bewältigung eines Vorfalls.

Der VSE begrüsst die Bestrebung, durch die Leistungen des NCSC die privatwirtschaftlichen Angebote nicht zu konkurrenzieren. Die zu erwartenden Unterstützungsleistungen des NCSC gemäss Art. 73a und Art. 74 Abs. 3 ISG sowie das Zusammenspiel zwischen dem NCSC als CERT für kritische Infrastrukturen und privaten Anbietern von CERT Dienstleistungen sind jedoch im Rahmen der Verordnung präziser festzulegen und

an die Erfordernisse für den Schutz kritischer Infrastrukturen anzupassen. Der VSE beantragt, dass das NCSC als GovCERT einen Schirm über die privatwirtschaftlichen CERTs bildet und diese bei der Krisenbewältigung je nach Situation und Bedarf unterstützt.

Art. 74 Abs. 3 ISG unterscheidet hinsichtlich des Zugangs zu Unterstützungsleistungen durch das NCSC zwischen privaten und nicht privaten Institutionen. Der Erläuternde Bericht schafft indes nicht hinreichend Klarheit über die sachlichen Beweggründe und Folgen dieser Unterscheidung. Verschiedene Betreiberinnen kritischer Infrastrukturen in der Strombranche sind Teil der öffentlichen Verwaltung, andere sind privatwirtschaftlich organisiert; sie weisen indes keine unterschiedlichen Gefährdungspotenziale auf. Die Trägerschaft oder Eigentumsverhältnisse sind somit als Unterscheidungskriterium nicht relevant und widersprechen dem Grundsatz, dass das NCSC nach Art. 73a Bst. f ISG alle Betreiberinnen von kritischen Infrastrukturen unterstützt.

Antrag:

Art. 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen

3 Es berät und unterstützt sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht ~~und, sofern es sich um private Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist~~.

Der Bundesrat unterstreicht in den Erläuterungen, dass auf Verordnungsebene zu präzisieren sei, aufgrund welcher Kriterien die Vorfälle nach Art. 74d ISG zu melden sind. Der VSE erachtet dies ebenfalls als notwendig. Insbesondere die Zuordnung nach Bst. b, ob ein fremder Staat einen Cyberangriff ausgeführt oder veranlasst hat, dürfte durch den Betroffenen nur schwer bis gar nicht durchführbar sein. Bezüglich Bst. d ist nicht klar, ob bereits das Auftreten früherer, möglicherweise gestoppter oder nicht erfolgreicher Angriffskomponenten meldepflichtig sind, oder nur solche, die direkt und unmittelbar für das Ziel des Cyberangriffs eingeführt wurden.

Nach Art. 73b Abs. 2 ISG können Informationen zu Cybervorfällen veröffentlicht oder an interessierte Behörden und Organisationen weitergeleitet werden, sofern dies dazu dient, Cyberangriffe zu verhindern oder zu bekämpfen. Der VSE anerkennt, dass solche Informationen hilfreich sein können, unterstreicht jedoch, dass Personendaten und Daten juristischer Personen nur mit ausdrücklicher und vorhergehender Zustimmung veröffentlicht werden sollen. In der Verordnung sollte zudem näher definiert werden, zu welchem Zeitpunkt Informationen veröffentlicht werden: Dies sollte ausschliessen, dass Betroffene, die verwundbar sind, durch Rückschlüsse für weitere Angriffe oder Straftaten exponiert werden.

Schliesslich weist der VSE darauf hin, dass Art. 24 revDSG für Vorfälle bezüglich Personendaten (mit hohem Risiko) eine Meldepflicht an den EDÖB vorsieht. Für denselben Vorfall kann es somit zu Meldungen an mindestens zwei verschiedene Behörden kommen. Betroffene Unternehmen sollten jedoch über den gleichen, vom NCSC koordinierten Kanal an den EDÖB melden können, sollte sich dies je nach Art des Angriffs als notwendig erweisen. Eine Doppelspurigkeit würde hingegen zu zusätzlichem Aufwand und schwierigen Abgrenzungsfragen führen.

Betreffend die Änderungen des StromVG begrüsst der VSE, dass sich der Bundesrat gemäss Erläuterndem Bericht beim allfälligen Erlass von Vorgaben für kritische Infrastrukturen der Strombranche auf Verordnungs-

stufe an den subsidiären Branchenregelungen orientieren will. Der VSE erachtet es als sinnvoll, wenn der Bundesrat die einschlägigen Branchennormen für anwendbar erklärt, da dies eine rasche Anpassung an die dynamische Entwicklung möglicher Bedrohungslagen und -szenarien ermöglicht. Beim allfälligen Erlass von Verordnungsbestimmungen muss das Gefährdungspotenzial im Hinblick auf die Versorgungssicherheit bei der Definition der einzuhaltenden Vorgaben und der Bezeichnung der verpflichteten Akteure berücksichtigt werden. Bei den Verordnungsbestimmungen ist sicherzustellen, dass ein pragmatischer Umgang mit der Meldepflicht gewählt wird, sodass auch kleineren und mittleren Unternehmen eine einfache und unkomplizierte Handhabung ermöglicht wird.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und unterstützen das NCSC gerne bei der weiteren Festlegung des effizienten Zusammenspiels von Akteuren im Ernstfall eines Cyberangriffs.

Für allfällige Rückfragen oder zur Diskussion stehen wir Ihnen gern zur Verfügung.

Freundliche Grüsse

Michael Frank
Direktor

Michael Paulus
Leiter Netze und Berufsbildung