Per Mail (PDF / Word) an:
ncsc@gs-efd.admin.ch
Eidgenössisches Finanzdepartement
3003 Bern

Bern, 14. April 2022

Stellungnahme der IG eHealth: Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrte Damen und Herren

Die IG eHealth nimmt gerne die Möglichkeit wahr, im Rahmen der Vernehmlassung zur Meldepflicht für Cyberangriffe für Betreiberinnen von kritischen Infrastrukturen (Revision Informationssicherheits-gesetz) Stellung zu beziehen.

Cyberattacken und Sicherheitsprobleme haben in der Vergangenheit zugenommen, z.B. bei meineimpfungen.ch, beim Transplantationsregister oder bei Primärsoftware im Kanton Neuenburg. Auch Lösegeldforderungen treten vermehrt auf. Der Handlungsbedarf ist also unbestritten.

Einleitende Bemerkungen

Im Grundsatz begrüsst die IG eHealth die Ergänzungen des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG). Namentlich die Verpflichtung wesentlicher Bereiche des Gesundheitswesens erachten wir als wichtig und richtig. Gemäss Art. 74b werden Spitäler, medizinische Laboratorien, Zulassungsinhaberinnen von Arzneimitteln oder Medizinprodukten und die Sozialversicherungen meldepflichtig. **Wir bitten das EFD/NSCS die Frage zu prüfen, weshalb Geburtshäuser und ambulante Anbieter wie Gruppenpraxen von Ärztinnen und Ärzten, Spitex-Organisationen oder Apotheken-Ketten und -Gruppierungen von der Meldepflicht ausgenommen sind?**

Konkrete Punkte

Aus Sicht der IG eHealth braucht es im Gesetz folgende Präzisierungen

Art. 5 Bst. d–e ISG Begriffe

Im Artikel werden die Begriffe Cybervorfall und Cyberangriff definiert. Im Gesetz wird verschiedentlich von Schwachstellen gesprochen, z.B. im Art. 73a Grundsatz.

⇒ Die Begriffe Cybervorfall, Cyberrisiko und Schwachstelle sind im Gesetz zentral, die Abgrenzung sollte präziser festgelegt werden. Wir bitten das EFD, den Begriff der Schwachstelle ebenfalls zu definieren und sich dabei an internationale Begrifflichkeiten zu halten (z.B. Common Vulnerabilities Scoring System CVSS).

Art. 73b Abs. 2 ISG Bearbeitung von Meldungen von Cybervorfällen und Schwachstellen

Die Veröffentlichung und Weiterleitung von Informationen zu Cybervorfällen können gegen Geschäftsinteressen verstossen. Die Frage, ob durch die Veröffentlichung und Weiterleitung Cyberangriffe verhindert oder bekämpft werden können, kann allenfalls erst nachträglich beurteilt werden.

⇒ Die IG eHealth schlägt zwei Punkte vor:

- es braucht im ISG einen Öffentlichkeitsvorbehalt, falls Geschäftsinteressen der Organisation / Firma betroffen sind, die den Mitbewerbern zu Vorteilen verhelfen oder zu einer Umsatzeinbusse führen könnten.
- Im ISG ist festzuhalten, dass die Meldung von Cybervorfällen, Cyberrisiken und Schwachstellen vom Geltungsbereich des Öffentlichkeitsgesetz BGÖ ausgenommen sind.

Art. 74d ISG Zu meldende Cyberangriffe

Ein Cyberangriff muss gemäss dem Gesetz immer gemeldet werden, wenn die Punkte a bis d erfüllt werden. Punkt b, wonach ein fremder Staat den Cyberangriff ausgeführt oder veranlasst hat, erachten wir als eher theoretischer Natur. Vielfach dürfte nicht ersichtlich sein, wer hinter dem Cyberangriff steht.

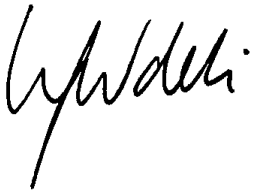
⇒ Die IG eHealth schlägt vor, Punkt d (Cyberangriff bleibt länger als 30 Tage unentdeckt) keiner Meldepflicht zu unterstellen, wenn die Punkte a (Funktionsfähigkeit gefährdet) und c (möglicher Abfluss oder zur Manipulation von Informationen) nicht erfüllt sind, d.h. der Angriff eine Bagatelle war oder einen tiefen bis mittleren Schweregrad aufwies.

Schlussbemerkungen

Die Vorgaben auf Gesetzesstufe sind genereller Natur. Bei der Ausarbeitung der Verordnungen ist es zentral, die betroffenen Akteure frühzeitig einzubinden. So sind der Meldeprozess und der Gegenstand und der Umfang einer Meldung klar zu definieren.

Der Bundesrat und das Parlament müssen sicherstellen, dass das Nationale Zentrum für Cybersicherheit NCSC genügend Personalressourcen erhält, um die vielfältigen Aufgaben bewältigen zu können. Ressourcen sind namentlich auch für die Unterstützung des NCSC bei Cybervorfällen und Schwachstellen vorzusehen, die im Art. 74 Abs. 3 ISG festgehalten ist. Wichtig ist auch, dass die Daten an die Behörden nur einmal erfasst und gemeldet werden müssen (Umsetzung Once-Only-Prinzip).

Besten Dank für die Kenntnisnahme und freundliche Grüsse



Anna Hitz
Präsidentin IG eHealth

Walter Stüdeli
Geschäftsführer IG eHealth

Die IG eHealth ist der einzige Fachverband mit Expertise in den Bereichen Gesundheitspolitik, Organisation, ICT, Semantik und Technik.

Sie unterstützt die digitale Transformation im Gesundheitswesen in der Schweiz proaktiv, damit Qualitäts- und Sicherheitslücken in der Behandlung abgebaut und administrative Prozesse verbessert werden.