santésuisse | Die Schweizer Krankenversicherer
Les assureurs-maladie suisses
Gli assicuratori malattia svizzeri

santésuisse
Römerstrasse 20
Postfach
CH-4502 Solothurn
Tel. +41 32 625 41 41
Fax +41 32 625 41 51
mail@santesuisse.ch
www.santesuisse.ch

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

Für Rückfragen:
Agnes Stäuble
Direktwahl: +41 32 625 4266
Agnes.Staeuble@santesuisse.ch

Solothurn, 12. April 2022

Vernehmlassungsverfahren zur Meldepflicht von Betreiberinnen und Betreibern kritischer Infrastrukturen für Cyberangriffe; Stellungnahme santésuisse

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, zur Einführung einer Meldepflicht für Cyberangriffe und der damit verbundenen Änderung des Informationssicherheitsgesetzes (ISG) Stellung nehmen zu können.

1. santésuisse erachtet eine entsprechende Meldepflicht als sinnvoll

Die Krankenversicherer sehen sich aufgrund der fortschreitenden Digitalisierung zunehmend mit Cyber-Bedrohungen konfrontiert. Es erweist sich daher als sachgerecht, mittels einer Meldepflicht bezüglich Cyberattacken ein Frühwarnsystem zu etablieren und dadurch eine bessere Übersicht zur Bedrohungslage zu schaffen und die Cybersicherheit zu stärken. Dementsprechend begrüsst santésuisse die vorgesehene Einführung einer solchen Meldepflicht für Cyberangriffe auf kritische Infrastrukturen.

2. Klärung von Begrifflichkeiten und Definitionen

- **Cyberrisiko**

  Der Begriff «Cyberrisiko» wird unseres Erachtens im vorliegenden Kontext nicht korrekt verwendet. Es müsste Cyberbedrohungen heissen. Das Risiko ist keine Bedrohung.

  Ein Unternehmen hat Schwachstellen die durch Bedrohungen aus dem Cyberraum ausgenutzt werden können. Das Risikoszenario beschreibt wie eine Schwachstelle durch die Bedrohung ausgenutzt werden kann. Das Risiko ist dann die Einschätzung der Eintrittswahrscheinlichkeit und des Schadenmasses für dieses Risikoszenario.

- **Art. 5 Bst. d E-ISG: Cybervorfall**

  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;

  Die hier gewählte Definition kann zu Missverständnissen führen. Solche Ereignisse können nämlich auch auftreten, ohne dass sie durch einen Cyberangriff ausgelöst werden, z.B. Ausfall von IT Komponenten oder Programmierfehler. Diese Ereignisse dürfen nicht unter die Meldepflicht fallen.

- **Art. 74d Abs. 1 Bst. b E-ISG**

  Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass ein fremder Staat ihn ausgeführt oder veranlasst hat.

  Die Zuordnung eines Angriffs zu einem ausländischen Staat ist eine besonders komplexe Aufgabe, für deren Durchführung die Krankenversicherer weder über die notwendigen Ressourcen noch über die erforderlichen Fähigkeiten verfügen. Im besten Fall kann ein solcher Angriff nur mit Unterstützung des NCSC gemeldet werden, d.h. das NCSC würde vor einer Meldung involviert werden, was keinen Sinn macht.

  Überdies sollte Art. 74d E-ISG präziser formuliert werden. Zusammen mit der betreffend Cybervorfall gewählten Definition in Art. 5 Bst. d E-ISG lässt der Artikel unseres Erachtens zu viel Spielraum offen für die Interpretation, was als meldepflichtiger Cyberangriff qualifiziert wird. Nicht klar zugeordnet werden können z.B. folgende Vorfälle:
  - DDoS Attacke: Diese ist für das Unternehmen spürbar. Der Service ist kurzzeitig nicht verfügbar, aber unter der in der BIA tolerierten maximalen Ausfallzeiten. Der Provider blockiert nach kurzer Zeit die Attacke.
  - Scans aus dem Internet, welche ausloten, ob ein Unternehmen verwundbare Systeme betreibt.
  - Vorhandene Software-Schwachstellen, die ausgenutzt werden können bis sie gepatched werden. Es gibt aber noch keine bekannten Exploits.
  - Phishing E-Mails, mit der Aufforderung auf einen Link zu klicken oder interne Informationen preiszugeben.

3. Es ist darauf zu achten, dass die administrative Belastung im Zusammenhang mit der Meldepflicht klein bleibt

Gemäss Art. 74a E-ISG sind die Betreiberinnen und Betreiber von kritischen Infrastrukturen gehalten, dem nationalen Zentrum für Cybersicherheit (NCSC) Cyberangriffe nach deren Entdeckung so rasch als möglich zu melden. Für die elektronische Übermittlung der Meldung stellt das NCSC ein sicheres System zur Verfügung (vgl. Art. 74f Abs. 1 E-ISG). Vor dem Hintergrund, dass die administrative Belastung im Zusammenhang mit der Meldepflicht möglichst klein sein sollte, unterstützt santésuisse die Zurverfügungstellung eines solchen Systems.

4. Verhältnis zu anderen Meldepflichten und Informationsaustausch unter den Behörden

Die Einführung einer Meldepflicht für Cyberangriffe tangiert bereits bestehende Meldepflichten, wie insbesondere die Meldepflicht nach Art. 24 des revidierten Datenschutzgesetzes (revDSG), wonach der Verantwortliche dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, zu melden hat.

santésuisse erachtet es auch im Verhältnis zu anderen Meldepflichten als wichtig, dass der Aufwand für die Erfüllung der jeweiligen Obliegenheit möglichst geringgehalten wird. Entsprechend befürworten wir, unter Gewährleistung des vollumfänglichen Datenschutzes, die vorgesehene Regelung betreffend die Weiterleitung der Meldung eines Cyberangriffs. Es soll den Meldenden offenstehen, die Meldung gleichzeitig mit der Übermittlung an das NCSC anderen Meldestellen weiterzuleiten, um damit anderweitige Meldepflichten zu erfüllen. Umgekehrt soll das NCSC auch Meldungen zu Cyberangriffen entgegennehmen, welche in Erfüllung einer anderweitigen Meldepflicht abgegeben wurden. Damit wird verhindert, dass Betroffene den gleichen Vorfall unterschiedlichen Stellen über unterschiedliche Verfahren melden müssen und dabei unterschiedlichen Meldepflichten mit divergierenden Meldeinhalten/Meldefristen für unterschiedliche Behörden zu berücksichtigen haben.

Vielen Dank für die Kenntnisnahme und Berücksichtigung unserer Anmerkungen. Für Fragen stehen wir gerne zur Verfügung.

Freundliche Grüsse

santésuisse

Direktion

Verena Nold
Direktorin

Rechtsdienst

Isabel Kohler Muster
Leiterin Rechtdienst santésuisse-Gruppe