digitalswitzerland | Waisenhausplatz 14 | 3011 Bern

Frau Ständerätin / Herr Ständerat
der Sicherheitspolitischen Kommission des Ständerats

Antwort auf den Entscheid des Nationalrats zum Geschäft 22.073 - Informationssicherheitsgesetz. Änderung (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen)

Sehr geehrte Damen und Herren Ständeräte,

Das neue Informationssicherheitsgesetz (ISG) ist ein wichtiger Meilenstein für die Cybersicherheit der Schweiz. Es ist zu begrüssen, da es dank der Meldepflicht für Cyberangriffe ermöglicht, ein viel schärferes Lagebild der Schweiz zu bekommen.

Der Gesetzesvorschlag, der vom Nationalrat am 16. März angenommen wurde, ist nicht abzulehnen, jedoch mit folgenden Anmerkungen zu ergänzen. Der Nationalrat möchte, dass nicht nur Cyberangriffe, sondern auch Schwachstellen gemeldet werden. Der Miteinbezug der Schwachstellen in die Meldepflicht hat jedoch zur Folge, dass Fragen entstehen, die einer Antwort bedingen und zwingend in den Gesetzgebungsprozess einfliessen müssen:

1. Ist die Cyberschwachstelle genau genug definiert, damit bei den Betroffenen ein einheitliches Verständnis besteht, welche Schwachstellen zu melden sind?
2. Welche Schwachstellen müssen gemeldet werden? Produkt- oder Implementierungsschwachstellen?
3. Können und sollen Schwachstellen der gleichen Meldelogik wie Cyberangriffe unterliegen?

Zur Frage 1:
Die ***Definition von Schwachstellen in der Gesetzesvorlage***, falls diese gemeldet würden, ist von Cybervorfällen nicht genau genug abgegrenzt:

- In der jetzigen Vorlage kann eine Schwachstelle so definiert werden, dass sie auf menschliches Versagen, beziehungsweise Implementierungsschwachstellen, zurückzuführen ist (Vgl. Art. 5g *Cyberbedrohung, die auf Schwächen oder Fehler in Informatikmitteln zurückzuführen ist).*
- Die unserer Ansicht nach ungenaue Definition der Cyberschwachstelle kann zu einer sehr hohen Anzahl an Meldungen von unterschiedlicher Qualität führen.
- Für die Definition von Schwachstellen wird folgender Vorschlag gemacht:
    - *Art. 5 lit g.: Schwachstelle: Cyberbedrohung, die auf Schwächen oder Fehler in Software- oder Hardwarekomponenten zurückzuführen ist.*
- Die Schwächen oder Fehler in Software- oder Hardwarekomponenten sind ***Produktschwachstellen***

Zur Frage 2
Unterscheidung zwischen Produktschwachstellen und Implementierungsschwachstellen:

- Eine Meldepflicht von Produktschwachstellen ist vorstellbar, aber schwer durchzusetzen (siehe unten, Meldelogik)
- Eine Meldepflicht von Konfigurations- oder Architekturfehlern (**Implementierungsschwachstellen**) macht unseres Erachtens keinen Sinn und führt zu einer Gefährdung des meldenden Unternehmens ohne Gewinn für die Allgemeinheit. Zudem ist davon auszugehen, dass zuerst der Implementierungsfehler behoben werden würde, und danach - wenn überhaupt - Meldung erstattet werden würde.

Zur Frage 3:

Bei der **Meldelogik und Durchsetzbarkeit der Meldefrist muss die Unterscheidung zwischen Produktschwachstellen und Cyberangriffen berücksichtigt werden.**

- Das Gesetz trägt der Unterscheidung von Cyberangriffen und -schwachstellen in der jetzigen Form nicht genug Rechnung. Cyberangriffe erfordern Mitigation und Abwehr, Schwachstellen erfordern Prävention. Entsprechend zeigen sich Unzulänglichkeiten bei Meldung und Bearbeitung, wenn Produktschwachstellen der gleichen Prozesslogik wie Cyberangriffe unterstellt sind.
- Entdeckt ein Schweizer Unternehmen eine Produktschwachstelle in einem Vendorprodukt, meldet es diese entweder bisher gar nicht oder dann direkt an den Hersteller selbst.
- Es existiert heute keine Meldepflicht zwischen Anwender und Hersteller. Neu wird aber eine Meldepflicht zu Dritten (NCSC) eingeführt. Dies schafft ein ambivalentes Vertrauensverhältnis. Im schlimmsten Fall entsteht ein Gefühl der Denunziation.
- Aus externer Sicht kann nicht festgestellt werden, wann eine Schwachstelle tatsächlich entdeckt wurde. Deswegen ist im Falle der Schwachstellen die Meldung innerhalb von 24 Stunden nicht beweisbar, beziehungsweise obsolet. Wie sollte überprüfbar sein, ob eine Meldung fristgerecht stattgefunden hat?
- Aus diesen Gründen schliessen wir uns der Haltung der Minderheit des Nationalrates an, dass eine Meldefrist von mindestens 72 Stunden eine Grundvoraussetzung für eine wirkungsvolle Umsetzung des Gesetzes ist.

Abschliessend sind wir der Meinung, dass eine umfassende Berichterstattung zum Gesetz notwendig ist. Es wäre beispielsweise abzuklären, ob:

- Eine Meldepflicht für Schwachstellen, wie sie momentan vorgesehen ist, in der Praxis durchsetzbar ist.
  - Gibt es Daten aus vergleichbaren Ländern?
  - Ist eine Meldepflicht von 24 Stunden für kleinere Unternehmen kapazitätsbedingt überhaupt umsetzbar?

Wir danken Ihnen für die Aufmerksamkeit. Für Fragen und Anmerkungen stehen das Cyber Security Committee sowie die Geschäftsstelle von digitalswitzerland jederzeit zur Verfügung.

Mit freundlichen Grüssen,

Stefan Metzger

Managing Director digitalswitzerland

stefan@digitalswitzerland.com

Guillaume Gabus

Public Affairs & Extended Management

guillaume@digitalswitzerland.com

Über digitalswitzerland

digitalswitzerland ist eine schweizweite, branchenübergreifende Initiative, welche die Schweiz als weltweit führenden digitalen Innovationsstandort stärken und verankern will. Unter dem Dach von digitalswitzerland arbeiten an diesem Ziel mehr als 200 Organisationen, bestehend aus Vereinsmitgliedern und politisch neutralen Stiftungspartnern, transversal zusammen. digitalswitzerland ist Ansprechpartner in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.