digitalswitzerland | Waisenhausplatz 14 | 3011 Bern

Frau Ständerätin / Herr Ständerat

Zürich, 26. Mai 2023

Informationssicherheitsgesetz - Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen (22.073)

digitalswitzerland unterstützt den Minderheitsantrag (Wicki, Bauer, Burkart, Français, Minder): Zustimmung zur Version des Bundesrats

Sehr geehrte Damen Ständerätinnen,
Sehr geehrter Herren Ständeräte,

Am 5. Juni 2023 werden Sie das Informationssicherheitsgesetz behandeln. digitalswitzerland sprach sich auch in Vergangenheit für die Einführung einer Meldepflicht für Cyber-Angriffe aus. Wir raten jedoch dazu, den Minderheitsanträgen zu folgen und die "Schwachstellen" in Art. 74 zu streichen, wie es der Bundesrat ursprünglich vorgeschlagen hatte. Diese Empfehlung stützt sich auf die folgenden Überlegungen:

1. In der Theorie ist die Meldelogik des Gesetzesvorschlages auf Cyberangriffe (Abwehr, Mitigation) und nicht auf Cyberschwachstellen (Prävention) ausgelegt - es sind konzeptionell zwei unterschiedliche Sachverhalte.
2. In der Praxis führt die Meldung von Schwachstellen zu weniger Kollaboration zwischen den Akteuren. Das Vertrauen wird nicht gestärkt, sondern eher geschwächt. Im Gegensatz zu Cyberangriffen, ist bei Schwachstellen die Frage, *was wann* den Behörden gemeldet werden muss, nicht genügend geklärt. Das *wer,* ist unserer Ansicht nach, in beiden Fällen noch nicht geklärt.

Aus oben genannten Gründen führt der Miteinbezug von Schwachstellen zu rechtlichen Fallstricken, die für Unternehmen und Behörden nicht absehbar sind und deshalb das Gesetz nicht umsetzbar machen.

Wir machen Sie auch darauf aufmerksam, dass wir das Schreiben und die darin enthaltenen Argumente der Betreiber der kritischen Infrastrukturen (Energie, Mobilität, Finanzen, Telekommunikation) vorbehaltlos unterstützen.

Erläuterungen:
Theorie:
Die identische Behandlung der Meldung von Schwachstellen und Cyberangriffen hat logische Unschärfen, die zu rechtlichen Fallstricken führen:

- Cyberangriffe sind fremdverschuldet, sie setzen einen Angriff von Aussen voraus - die Reaktion darauf ist Abwehr und Mitigation.
- Schwachstellen sind unbewusst selbstverschuldet, es handelt sich also um Fehler, für welche die Verantwortung zwischen dem Produkthersteller und dem Anwender liegt, ohne Einwirkung von Aussen - das Rezept dafür ist Prävention und Kollaboration

Der Miteinbezug von Schwachstellen führt dazu, dass das Gesetz, weil es zwei verschiedene Sachverhalte auf die gleiche Art behandelt, nicht praktikabel ist.

Praxis:
In der Praxis zeigen sich gleich mehrere Probleme auf:

- *Was wird gemeldet*: Die Definition von Schwachstellen ist unscharf. Das Gesetz präzisiert nicht, um welche Schwachstellen es sich handelt; z.B. Produktschwachstellen wie Software-, Hardware-, und Netzwerk-Fehler, oder Implementierungsschwachstellen wie Konfigurations-fehler, physische Schwachstellen (z.B ungesicherte Räumlichkeiten) oder menschliche Fehler (z.B. ein zu schwaches Passwort). Die Meldung von Implementierungsschwachstellen führt zu einer Gefährdung des meldenden Unternehmens ohne Gewinn für die Allgemeinheit.
- *Wer muss melden:* Während bei Angriffen ein Anreiz besteht, eine Meldung abzugeben, ist nicht klar, welche und wie viele Organisationen als Betreiber von kritischen Infrastrukturen gelten. ***Es sollte zuerst geklärt werden, wie viele und welche Organisationen von einer Meldepflicht betroffen sind.***
- *Wann wird gemeldet:* Es kann aus externer Sicht nicht festgestellt werden, wann irgendeine Schwachstelle tatsächlich entdeckt worden ist. ***Eine fristgerechte Meldung ist nicht beweisbar.***
- *Wie wird heute mit Schwachstellen umgegangen:* Die gängige Praxis ist folgende: häufig veröffentlichen ICT-Anbieter Sicherheitsbulletins und -hinweise, um Kunden rechtzeitig über bekannte Schwachstellen, Patches und Umgehungslösungen für ihre Softwareprodukte zu informieren. Diese Unternehmen würden künftig von den Sanktionen im Gesetz erfasst. Entdeckt ein Anwender heute eine Schwachstelle, meldet er dies dem Anbieter und es wird bilateral nach Lösungen gesucht.
- *Wie würde zukünftig gemeldet werden:* Das Gesetz fordert eine Meldung an einen Dritten (NCSC), obschon die Verantwortung für die Schwachstelle und deren Behebung zwischen dem Hersteller und/oder dem Anwender liegt. Es ist, als wenn man bei Hinweisen auf Fehler via E-Mail immer mit “reply-all” antworten würde - das Vertrauensverhältnis zwischen Kunde und Anbieter würde belastet.

Wir danken Ihnen für die Aufmerksamkeit. Für Fragen und Anmerkungen steht Ihnen 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.