SSK | CMP
Schweizerische Staatsanwaltschaftskonferenz SSK
Conférence suisse des Ministères publics CMP
Conferenza svizzera dei Ministeri pubblici CMP

An
Bundesamt für Cybersicherheit BACS
3003 Bern

Per E-Mail
ncsc@ncsc.admin.ch

Bern,13. September 2024

Vernehmlassung Cybersicherheitsverordnung (CVS) – Stellungnahme SSK

Sehr geehrte Damen und Herren

Mit Schreiben vom 22. Mai 2024 haben Sie unsere Konferenz eingeladen, zur erwähnten Vorlage Stellung zu nehmen. Hierfür danken wir Ihnen bestens.

Fristgerecht möchten wir uns gerne zu folgenden Punkten äussern:

- **Schnittstelle BACS zu den Strafverfolgungsbehörden**

Gemäss den Erläuterungen zur Verordnung über die Cybersicherheit vom 22. Mai 2024 zur Vorfallsbewältigung (nachfolgend Erläuterungen), soll das nationale Computer Emergency Response Team (CERT) des BACS eine zentrale Rolle spielen bei der Bewältigung von Cybervorfällen und Cyberbedrohungen in der Schweiz. Das BACS arbeite dabei eng mit den betroffenen Behörden und Organisationen und ihren allfälligen Sicherheitsdiensten zusammen. Es helfe zudem bei der Koordination zwischen den an der technischen Bewältigung beteiligten Akteuren.

Mit Bezug auf die technische Vorfallsbewältigung ist das CERT eine längst (seit Schaffung MELANI) etablierte Stelle mit sehr gutem Fachwissen und grossem Netzwerk. In den Erläuterungen zu Art. 7 CSV ist die Zusammenarbeit mit den Strafverfolgungsbehörden aber nicht explizit erwähnt. Es ist fraglich und offen, ob mit betroffenen Behörden auch die Staatsanwaltschaft und die Polizei gemeint sind.
Wichtig ist bei Vorfällen die zeitnahe Involvierung der Strafverfolgungsbehörden. Es besteht üblicherweise Gefahr im Verzug zur Sicherung der nötigen Beweise. Zudem können Sicherungsmassnahmen der Betroffenen oder des CERT die forensische Erhebung von Beweismitteln vereiteln, da die Daten durch vorgängig vorgenommene Manipulationen kompromittiert wurden, was einen faktischen oder rechtlichen Beweisverlust zur Folge haben kann.
Gerade bei Offizialdelikten ist für den Erfolg einer Strafuntersuchung zentral, dass die betroffenen Behörden zeitnah informiert werden.

Unseres Erachtens sollten die in der Praxis durchaus vorhandenen Kontakte des BACS (CERT) zu den Strafverfolgungsbehörden in der Verordnung institutionalisiert (vgl. Ausführungen auf Seite 2) **und in den Erläuterungen beschrieben werden.**

Bezüglich der Zulässigkeit von in den Erläuterungen mehrfach erwähnten Gegenmassnahmen (S. 11, 15 und 17) bestehen unterschiedliche Auffassungen und ein rechtlich enger Rahmen. Demgegenüber ist technisch sehr vieles möglich. Es ist zu definieren, was das CERT unter Präventiv- und Gegenmassnahmen versteht.

Je nach Verständnis und Umfang sind erweiterte gesetzliche Grundlagen erforderlich für Massnahmen, welche in der Regel nur den Strafverfolgungsbehörden gemäss StPO oder dem Nachrichtendienst gemäss NDG offenstehen.

Wir schlagen deshalb vor, Gegenstand, Wirkungsziele und Umfang der «Gegenmassnahmen» zu definieren und die dafür nötigen Kompetenzen des CERT zu umschreiben.

- **Weitergabe von Informationen Gemäss Art. 15 CSV**

Laut Entwurf von Artikel 15 CSV soll das BACS über die Weitergabe der Informationen frei entscheiden können. Diese Kompetenz steht im Spannungsfeld zum Informationsbedarf der Strafverfolgungsbehörden. Dass ein vertrauensbasierter Informationsaustausch mit den Informationslieferanten schützenswert ist, ist anzuerkennen. Eine effektive Strafverfolgung ist aber ohne zeitnahe Informationen nicht möglich. Im Ergebnis und angesichts der betroffenen Rechtsgüter sind öffentliche Interessen, namentlich Strafverfolgungsinteressen, höher zu gewichten als das Selbstbestimmungsrecht des BACS. Immerhin sind die Informationen bei den Strafverfolgungs-behörden durch das Amtsgeheimnis geschützt und werden nur zweckgebunden verwendet.

Wir regen deshalb an, die in Art. 15 Abs. 2 CSV vorgeschlagene Kompetenz über die Weitergabe von Informationen so weit zu beschränken, als sie die vollständige Übermittlung der Informationen an die Strafverfolgungsbehörden betrifft.

- **Meldepflicht für Betreiber kritischer Infrastrukturen gemäss Art. 18 Abs. 4 CVS / Kannvorschrift Anzeigenerstattung Direktor BACS gemäss Art. 73d Abs. 3 ISG**

Laut des erläuternden Berichts sollen das revidierte Kapitel 5 des Informationssicherheitsgesetz ISG und die Cybersicherheitsverordnung gleichzeitig per 1. Januar 2025 in Kraft treten. Mitarbeitende des BACS sind gemäss Art. 73d Abs.3 ISG von der Anzeigepflicht nach Art. 22a Abs. 1 BPG befreit und melden Hinweise auf eine mögliche Straftat ausschliesslich der Direktorin oder dem Direktor des BACS. Dieser wiederum **kann** Anzeige bei den Strafverfolgungsbehörden erstatten, **«sofern dies aufgrund der Schwere der möglichen Straftat geboten scheint.»**

Aus Sicht der Strafverfolgung ist die Anzeigenerstattung durch das BACS bei Cyberangriffen auf kritische Infrastrukturen bei möglichen Vergehen oder Verbrechen **imme**r geboten – geht es letztlich um die Sicherheit des Landes. Die Erläuterungen zur Verordnung führen denn auch aus, welche gravierende Folgen bis hin zu Sicherheitsrisiken meldepflichtige Cyberangriffe haben können und begründen die Meldepflicht im Sinne von Art. 18 Abs. 4 CSV damit, dass das BACS müsse einschätzen können, «wie stark die Bedrohung kritischer Infrastrukturen durch Cyberkriminelle ist» (S. 27 und 28).

Die Übersicht über die Cyberkriminalität in der Schweiz ist lückenhaft, die Dunkelziffer hoch. Privatpersonen und Unternehmen wird denn auch oft vorgeworfen, dass sie Cyberangriffe nicht melden, was wiederum die Arbeit der Strafverfolgungsbehörden von Bund und Kantonen im Kampf gegen die Cyberkriminalität erschwer. Dass selbst das für Cybersicherheit verantwortliche Bundesamt solche Angriffe nicht anzeigt, erachten wird als widersprüchlich.

Wir schlagen deshalb vor, Art. 18 CSV mit einem Absatz 5 zu ergänzen, wonach das BACS (zumindest) **Fälle im Sinne von Absatz 4 den zuständigen Strafverfolgungsbehörden zur Anzeige bringt.**

- **Kein Vertretungsmonopol BACS**

In Artikel 15*a* Absatz 2 Buchstabe h OV-VBS wird neu aufgeführt, dass das BACS die Schweiz zur technischen Analyse von Cyberbedrohungen und zur Bewältigung von Cybervorfällen in internationalen Gremien vertritt. Gemäss den Erläuterungen (S. 33) dient dieser Informationsaustausch dazu, relevante Erkenntnisse und Daten über aktuelle Bedrohungen zu teilen und gemeinsame Massnahmen zur Bewältigung von Cybervorfällen und Cyberbedrohungen zu koordinieren. Der nationale und internationale Austausch zwischen Fachstellen sei deshalb für den Schutz vor Cybervorfällen und Cyberbedrohungen unerlässlich. Das BACS tausche diesbezüglich aktiv Informationen mit inländischen und internationalen Stellen aus, die ähnliche Aufgaben wie das BACS wahrnehmen würden.

Weder Art. 15a Abs. 2 Bst. h OV-VBS noch die Erläuterungen umschreiben, wie weit dieses Vertretungsmonopol geht. Die Polizei nimmt im Bereich Cyberbedrohungen ähnliche Aufgaben wahr, auch die Staatsanwaltschaften bewältigen Cybervorfälle. Der nationale und internationale Austausch zwischen Strafverfolgungsbehörden ist längst etabliert.

Der Umfang, in welchem das BACS die Gremienarbeit vornimmt, ist unseres Erachtens genauer zu definieren und auf den Bereich Cybersicherheit zu beschränken. Der nationale und internationale Austausch der Strafverfolgungsbehörden präventiv zum Schutz vor Cyberbedrohungen sowie repressiv zur Bewältigung von Cybervorfällen darf durch diese Bestimmung nicht eingeschränkt werden.

Für die Berücksichtigung unserer Anliegen danken wir bestens.

Mit freundlichen Grüssen

Michel-André Fels, Präsident

Kopie

Mitglieder SSK-CMP