December 23 2022

Federal Council submits dispatch and draft law on mandatory reporting of cyberattacks on critical infrastructures

Walder Wyss Ltd | Tech, Data, Telecoms & Media - Switzerland

JÜRG SCHNEIDER

FLORIAN ROTH

According to a press release dated 2 December 2022 (available in English, German, French and Italian), the Federal Council has submitted a dispatch (the Federal Council dispatch) along with a draft bill of law to Parliament that will introduce a mandatory reporting of cyberattacks on critical infrastructures in Switzerland. The legal basis for this new reporting obligation will be created by an amendment to the Information Security Act (ISA). The amendment also brings about additional competencies for the Swiss National Cyber Security Centre (NCSC).

ISA as approved by Parliament in December 2020

The original version of the new ISA was adopted by Parliament on 18 December 2020 (for further details, see "Parliament adopts Information Security Act"). Rather than setting out detailed obligations and standards itself (which could be quickly outdated), the ISA is designed as an overarching law establishing a harmonised framework within which the competent federal authorities in the relevant sectors can implement adequate information security measures through ordinances and directives. The framework law provides, in particular:

- risk management procedures;
- uniform information classification categories;
- security checks on people; and
- federal support for operators of critical infrastructures in the field of information security.

The ISA applies, among other things, to:

- centralised and decentralised government agencies;
- public and private organisations outside the federal administration entrusted with administrative tasks; and
- public or private organisations operating critical infrastructures.[(1)]

The ISA as adopted by Parliament is expected to enter into force mid-2023, whereby the exact date is yet to be determined by the Federal Council.

On 24 August 2022, the Federal Council opened a public consultation for a series of new ordinances designed to implement the ISA, in particular the new Information Security Ordinance (ISO) (for further details, see "Information Security Act: Parliament approves draft").[(2)]

The ISA as adopted by Parliament did not provide for a reporting obligation of cyberattacks on critical infrastructures. Critical infrastructures comprise drinking water and energy supply, information, communication and transport infrastructures, as well as other processes, systems and facilities that are essential for the functioning of the economy and the well-being of the population.[(3)]

On 12 January 2022 (ie, even before the ISA entered into force), the Federal Council initiated a public consultation procedure on an amendment of the ISA providing in particular for the introduction of a duty to report cyberattacks on critical infrastructures (for further details see "Federal Council opens consultation on introduction of critical infrastructure cyberattack reporting obligation"). The consultation was completed on 14 April 2022.

New reporting obligation pursuant to draft law

Upon receiving positive feedback in the public consultation proceedings, on 2 December 2022, the Federal Council decided to implement the proposed duty to report cyberattacks on critical infrastructures and entrust the NCSC with additional tasks in a draft bill of law and a Federal Council dispatch (available in German, French, and Italian) submitted to Parliament.

The reporting obligation only applies to:

- to certain operators of critical infrastructures as defined in article 74b of the draft bill; and
- to cyberattacks with a significant damaging potential as defined in article 74d of the draft bill – namely, attacks that:
  - threaten the effective functioning of critical infrastructures;
  - led to a manipulation or breach of information;
  - remained undetected for a longer period of time, in particular if there are indications that the attack served as a preparation for further attacks; or
  - are associated with extortion, threats or coercion.

Notice must be submitted within 24 hours after the attack is detected.

The main reason for introducing a duty to report cyberattacks against critical infrastructures is to ensure early-stage warning and improve the visibility of ongoing threats. As perpetrators of cyberattacks often use similar methods and patterns for several critical infrastructures in different sectors, this obligation can significantly enhance the cybersecurity of critical infrastructures through early identification of attack methods and transmission of corresponding warnings.[(4)]

The draft bill presents a reporting obligation that replaces the current legal framework based on voluntary reporting of cyberattacks. The Federal Council feared that voluntary reporting would lead to an incomplete picture of threats since only a small part of (the increasing number of) operators of critical infrastructures will interact with the NCSC on a regular basis.[(5)]

A key concern raised during the consultation phase was that the reporting obligation should not result in a large additional administrative burden. In order to make reporting as simple as possible, the NCSC will provide an electronic reporting form. Furthermore, reporting modalities will be designed such that companies can simultaneously address reporting obligations arising under several Swiss laws with one notice. Companies reporting a cyberattack may choose to share the notice with other Swiss authorities – for example, with the Swiss Data Protection Officer to fulfil their obligation to report a data breach or loss under article 24 of the revised Swiss Data Protection Act (entering into force on 1 September 2023).

Enforcement

The reporting obligation will be enforced on the one hand with positive incentives and, on the other hand, with sanctions in case of violations. The NCSC offers first responder technical support with the management of the cyber incident, which is intended to incentivise organisations to cooperate with the NCSC. Violations of the reporting obligations may be sanctioned with a fine of up to 100,000 Swiss francs per incident. However, when the NCSC becomes aware of a cyber incident and sees that a reporting obligation may apply but no report is received from the relevant organisation, it will remind the organisation to report the incident before a fine is imposed against the natural persons responsible for the failure (article 74g and 74h of the draft bill). In cases where a fine of no more than 20,000 Swiss francs seems adequate, the organisation itself (instead of the responsible natural persons) may be sanctioned with the fine.

New tasks for NCSC

In order to enhance Switzerland's cybersecurity resilience and in particular implement the above-mentioned cyberattack reporting obligation, the draft bill entrusts the NCSC with a variety of new tasks (article 73a(2) of the draft bill), which include:

- raising awareness of and warning against cyber risks among the general public;
- warning authorities, organisations and persons in case of imminent cyberthreats and ongoing attacks;
- publishing information on cybersecurity and instructions on preventive and reactive measures to be taken against cyber risks;
- receiving and processing reports on cyber incidents and cyberthreats; and
- supporting operators of critical infrastructures, in particular, as a first responder in cases of a cyberattack.

The Federal Council recognises that these new tasks will significantly increase the NCSC's workload, and that an increase in staffing may be necessary.[(6)]

Comment

It is recommended that operators of critical infrastructures closely follow the described regulatory developments and put in place the necessary processes to ensure compliance with the upcoming reporting obligation once it enters into force.

For further information on this topic please contact Jürg Schneider or Florian Roth at Walder Wyss by telephone (+41 58 658 58 58) or email (juerg.schneider@walderwyss.com or florian.roth@walderwyss.com). The Walder Wyss website can be accessed at www.walderwyss.com.

Endnotes

(1) Article 2 of the ISA in conjunction with article 2 of the Government and Administration Organisation Act 21 March 1997 (SR 172.010).

(2) The documentation on the public consultation is available here (in German).

(3) Article 5 lit c of the ISA.

(4) Page 16 of the Federal Council dispatch.

(5) Page 6 of the Federal Council dispatch.

(6) Page 57 of the Federal Council dispatch.