International Law Office

February 4 2022

Federal Council opens consultation on introduction of critical infrastructure cyberattack reporting obligation

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

JÜRG SCHNEIDER

HUGH REEVES

ASHLEY ROBINSON

On 12 January 2022, the Federal Council initiated a consultation procedure with the cantons, political parties and the business sector on the introduction of a duty to report cyberattacks on critical infrastructures and the resulting amendment to the Information Security Act (ISA).[(1)] The consultation is open until 14 April 2022.[(2)]

In order to combat the increasing impact of cyberattacks perpetrated on Swiss authorities and companies – the National Cybersecurity Centre (NCSC) registers over 300 attempted or completed cyberattacks weekly – the project focuses essentially on two main axes:

- an obligation to report cyberattacks; and
- new tasks for the NCSC in supporting the economy and the general public.

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. For reference, critical infrastructures comprise water and energy supply, communication and transport infrastructure, and other facilities, processes and systems essential to the functioning of the economy and the wellbeing of the population. However, the reporting obligation only applies to cyberattacks with a significant damaging potential – ie, attacks that threaten the effective functioning of critical infrastructures or are associated with extortion, threats or coercion. Such reporting shall be made to the NCSC using a standardised form.

In order to protect Switzerland against cyber risks, the project also entrusts the NCSC with several new tasks, which include:

- raising awareness of cyber risks among the general public;
- warning of cyber risks and vulnerabilities in information technology;
- publishing information on cyber security and instructions on preventive and reactive measures to be taken against cyber risks; and
- supporting operators of critical infrastructures, in particular as a first aid service in cases of cyberattack.

Furthermore, the project recognises that these new tasks will significantly increase the NCSC's workload, and that an increase in staffing will be required accordingly.

As such, the project in consultation represents an important milestone in the implementation of the national strategy for the protection of Switzerland against cyber risks, and it would become, if implemented in the ISA, a welcome step in the right direction.

For further information on this topic please contact Jürg Schneider, Hugh Reeves or Ashley Robinson at Walder Wyss by telephone (+41 58 658 58 58) or email (juerg.schneider@walderwyss.com, hugh.reeves@walderwyss.com or ashley.robinson@walderwyss.com). The Walder Wyss website can be accessed at www.walderwyss.com.

Endnotes

(1) Parliament approved the ISA in December 2020. The Federal Council will set a date for its entry into force.

(2) The official announcement is available in German, French, Italian and English. Anyone wishing to participate in the consultation process is invited to send their observations (in Word and PDF) to ncsc@gs-efd.admin.ch by 14 April 2022.