TECH, DATA, TELECOMS & MEDIA - SWITZERLAND

Federal Council moves forward in protection against cyber risks

12 June 2020 | Contributed by Walder Wyss

AUTHORS

Jürg Schneider

Hugh Reeves

Ashley Robinson

On 27 May 2020 the Federal Council adopted the Ordinance on Protecting against Cyber Risks (OPCy, available in French and German), which is set to enter into force on 1 July 2020. This move is the next step in a series of measures taken by the Federal Council to adopt a new organisational structure and implement a national strategy to protect Switzerland against cyber risks (NCS, available in German, French, Italian and English).

The OPCy regulates the structure and tasks of several cybersecurity bodies of the federal administration. A so-called 'Cyber Group' (Article 8 of the OPCy) is composed of representatives from several federal departments, a representative of the cantons and is presided over by the federal cybersecurity delegate. The Cyber Group's tasks mainly focus on the assessment of cyber risks and existing mechanisms in the fields of cybersecurity, cyber defence and cybercrime. It also supports the interdepartmental management of cyber incidents.

Moreover, the OPCy provides for the development of a National Cyber Security Centre (NCSC) – also headed by the federal cybersecurity delegate and encompassing the existing structure known as MELANI – that will coordinate Switzerland's efforts in the field of cybersecurity and whose tasks will namely include:

- operating a national contact point on cyber risks that centralises and analyses reports from the federal administration, economic sectors, cantons and general population;
- running the national Computer Emergency Response Team (GovCERT);
- managing the federal administration's specialised IT security service; and
- assisting different offices in implementing the NCS and developing, implementing and evaluating standards and regulations in the field of cybersecurity.

The NCSC also manages cyber incidents that threaten the functioning of the federal administration, in which case it can obtain all necessary information from the service providers and beneficiaries in question and take emergency measures. Under Article 12(2) of the OPCy, the NCSC may also process data relating to cyber incidents that is useful, even indirectly, to the protection of the federal administration against cyber risks.

Notably, the OPCy further regulates some compliance aspects with regard to external service providers mandated by federal administrative units. Federal administrative units must integrate cybersecurity directives – presumably those enacted by federal cybersecurity institutions – in their contracts with external service providers (Article 14 of the OPCy). In such contractual relationships, the provider must inform the beneficiary of detected vulnerabilities or cyber incidents and the parties must define together a process for managing cyber incidents. Moreover, should this process fail to resolve a cyber incident, the affected parties must inform the NCSC to establish the appropriate course of action.

Along with the adoption of the OPCy, the Federal Council has also planned for 20 additional positions in the respective offices for cyber risk protection. With already 24 new positions approved in May 2019, this commitment to increase available resources and institutional centralisation reflects a welcome development in the strengthening of cyber security in Switzerland.

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.

disclaimer.