October 22 2021

Switzerland's 2018-2022 national strategy for the protection against cyber risks: implementation is on track

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

JÜRG SCHNEIDER

HUGH REEVES

ASHLEY ROBINSON

Introduction

On 17 August 2021, the Federal Council's cyber committee adopted the report (available in French, German and Italian) on the progress made in implementing the 2018-2022 national strategy for the protection of Switzerland against cyber risks (NCS).

The National Cyber Security Centre (NCSC) coordinates the implementation of the NCS and releases an annual progress report. The latest report shows the status of implementation as of the second quarter of 2021. The implementation of the NCS is proceeding according to plan. Roughly half of the milestones have been reached, and a fifth of the measures are now fully implemented.

Organisational structures

The implementation of the NCS includes the creation of organisational structures at the federal level. The NCSC has been operating a national desk for cyber risks since 1 January 2020. In 2020, some 10,834 reports were received from companies and individuals. Of the cases with a clear cybercrime component, 5,924 (55%) were fraud attempts, 416 (4%) were malware, 165 (2%) were due to hacking and 24 (less than 1%) were due to data leaks. As part of the overall strategic plan of the NCS, the Federal Department of Defence, Civil Protection and Sport adopted a cyber strategy which sets out the direction for cyber defence for the years 2021 to 2024. In the area of criminal prosecution, the Conference of Cantonal Directors of Justice and Police has concluded an administrative agreement for the organisation and financing of a national network for investigative support in the fight against cybercrime.

Vulnerability management and security labels

The NCSC has continued to grow and new services have been introduced. The development of vulnerability management is underway. A successful pilot test was conducted to identify potential vulnerabilities in federal government systems with the help of ethical hackers. In the context of the SwissCovid app and the COVID certificate, the NCSC carried out two public security tests, enabling the entire federal administration to benefit from its expertise.

With the increasing progress of digitalisation, small and medium-sized enterprises (SMEs) are ever more exposed to cyberthreats. In addition, Swiss SMEs are increasingly turning to external IT service providers. Indeed, two thirds of SMEs now work with such providers. As these providers have a direct impact on the cyber resilience of SMEs, it is essential that they have technical and organisational competence in cyber and information security. In the fourth quarter of 2020, partners from the federal government and the private sector took the initiative to create an independent quality label for IT service providers. This quality label will designate IT service providers that have adopted technical and organisational measures to ensure an adequate level of protection for their customers. The distribution of this label will have a positive influence on the cyber resilience of SMEs, raise the quality level of digital transformation activities and thus strengthen the trust placed in Switzerland in the field of digital security.

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.