International Law Office

May 27 2022

# National Cyber Security Centre: key updates

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

JÜRG SCHNEIDER

HUGH REEVES

KILIAN BOSSON


- NCSC to become federal office
- Report on information security


This article discusses two key updates about the National Cyber Security Centre (NCSC):

- the Federal Council, which is the Swiss executive body, recently announced that the NCSC will become a federal office; and
- the NCSC released its half-year report on information and cybersecurity incidents.

**NCSC to become federal office**

In a press release dated 18 May 2022, the Federal Council announced that the NCSC will become a federal office.

With a staff of approximately forty people, the NCSC is responsible for key tasks in protecting Switzerland against cyber threats. However, in view of the growing importance of cybersecurity, the NCSC's mandate is constantly expanding and becoming more relevant. After considering various options, the Federal Council decided to turn the NCSC into a full-fledged federal office, within one of the seven federal departments. The NCSC will therefore stay within the central federal administration and will see its structural standing reinforced, thereby further enabling any future growth. The modalities of this next chapter in the NCSC's development remain open and subject to internal analysis and proposals to the Federal Council, expected by the end of 2022.

**Report on information security**

On 5 May 2022, the NCSC published its report regarding information security and the most important cyber incidents of the second half of 2021 (available in French, German, Italian and English). In the NCSC's report, special attention is given to the attacks on IT product supply chains, which have recently caused various incidents in Switzerland. It also presents the main threats and cases of cyber incidents identified in Switzerland and abroad during 2021.

As the report explains, many companies rely on partner products or services to deliver their services. These companies are therefore entirely dependent on external services to maintain their business offerings. An attack through the supply chain can then reach a large number of victims, as the original suppliers of such services serve as gateways for attackers to lower levels of the chain. The most notable example of this type of attack in 2021 is probably the distributed denial-of-service attack that temporarily took down, among other things, the website of the canton of St Gallen.

The report also outlines various threats and cyber incidents identified in Switzerland in 2021. Among the four main vulnerabilities detected, the report mentions the critical vulnerability discovered in Log4j, a popular Java library providing logging infrastructure to third-party applications. In addition, two major data leaks were recorded:

- Fortinet VPN Credentials, which affected some 400 entries related to Switzerland; and
- EasyGov, where the names of some 130,000 companies that used covid-19 loans were stolen.

More specifically, in the area of social engineering and phishing, the NCSC has observed a mutation in phishing attempts, which are increasingly based on local companies and less on large international brands. In this context, criminals are now using tailored methods to attack very specific targets. The NCSC therefore recommends vigilance and caution, even in seemingly familiar situations.

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