TECH, DATA, TELECOMS & MEDIA - SWITZERLAND

Latest MELANI report – most important cyber incidents in second half of 2019

05 June 2020 | Contributed by Walder Wyss

On 30 April 2020 the Reporting and Analysis Centre for Information Assurance (MELANI) published its latest semi-annual report regarding the most important cyber incidents and cyber risks of the second half of 2019 in Switzerland and abroad. The latest report also contains a section reminding that the safe processing of data on the Internet is a priority for MELANI. The report is available in English, German, French and Italian. A technical appendix is available in English only.

Every six months, MELANI publishes a report regarding the latest cyber incidents and cyber risks in Switzerland and internationally. In this respect, MELANI follows the most recent developments abroad and highlights some of the incidents that have been brought to its attention in recent months. Moreover, the report contains several practical recommendations for individuals and companies to improve their protection against cyberattacks.

The general focus of MELANI's latest report pertains to data protection. The report highlights the ever-increasing risks to personal data, citing numerous data leaks and loss (technically, copies) of personal data, including patient medical data (sensitive personal data).

With regard to Switzerland, some noteworthy incidents in the second half of 2019 may be summarised as follows:

- Continued cyberattacks against sports organisations based in Switzerland. In this respect, the Organising Committee for the Olympic and Paralympic Games has warned against email campaigns that misrepresent its identity in order to lead recipients to phishing pages or infect their devices.
- Use of CEO fraud against Swiss companies. Fraudsters pass themselves off as company personnel and contact the HR department to request that employee salaries be paid into a different bank account. The fraudsters use free messaging services as well as data from employees that are freely available to commit this fraud.
- Various scams relating to online money placement. In this context, some fake online trading platforms promise fast and large gains in cryptocurrencies by misusing the image of personalities (eg, Roger Federer) and using social networks to reach a large public of potential investors.
- The growing threat of ransomware. For instance, a Swiss football club and a public transport company were victims of ransomware attacks. In this respect, the football club was prevented from selling match tickets while the traffic of the public transport company was slightly disrupted.
- Fake online stores. In the second half of 2019 alone, 450 such websites were blocked by the Zurich cantonal police, with the collaboration of SWITCH, which manages the '.ch' country code top-level domain.
- The challenge posed by the Emotet malware. This malware contains a Trojan horse which recovers the contents of previous email exchanges and uses them to generate new messages which are sent to all contacts in recipient lists. These emails come with an attachment, usually a Word file containing a malicious macro. As soon as a recipient opens this file and activates the edit mode, the macro runs and, save for additional protection, enables Emotet to download additional modules and remain on the victim's computer. Access to the corrupted system can then be sold to third parties.

Moreover, the report lists various measures which were or will be introduced to strengthen cybersecurity in Switzerland. These include the following measures:

- The Federal Office for National Economic Supply recently published the brochure Minimum Standard to Secure Information and Communication Technology in the Food Chain to help companies in the sector to avoid computer breakdowns or resolve them quickly when they occur; and

AUTHORS

Jürg Schneider

Hugh Reeves

Christophe Gösken

- The Swiss National Cybersecurity Centre's development of a bug bounty policy, which sets out rules on the responsible disclosure of security vulnerabilities and other such risks.

The report provides an overview of cybersecurity in Switzerland and abroad as well as technical recommendations for reducing certain risks. Nevertheless, legal issues are not addressed in this document and it is still necessary to remain appraised of the ongoing legal developments in this respect.

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