Digitalisation | e-government

Cybersecurity – challenges for political Switzerland

State of the art

Digitalisation is the collective term for the increasingly extensive and unavoidable use of information and communication technologies in society and the economy. In the simplest case, digitalisation can mean the direct replacement of manual or paper-based processes with electronic ones. However, most digitalisation projects should improve existing processes or enable ones to be implemented that were previously not feasible or too expensive.

If digital processes change significantly, the individual working methods, cooperations and even the professions and jobs of users, who do not generally have specialist IT knowledge, will also change. The term «digital transformation» is often used in this context to indicate that such projects are not purely IT projects, but also depend on close interaction between IT and users for the definition, drawing up and implementation of such projects. Countries such as Estonia, Latvia, Norway and Sweden are already well advanced at national level and their business and administration processes are largely paperless – cash has also been replaced by digital payment methods. In Switzerland, a conservative outlook in society, high expectations in terms of IT security and privacy, and firmly established federalism mean a more cautious, graduated and fragmented approach is being adopted, especially by authorities and administrations. Projects such as E-ID, e-Voting and the electronic patient record provoke contentious debate.

Recommendations

An important milestone was reached in 2019 with the creation of the position of a Federal Cyber Security Delegate. Ueli Maurer, the President of the Swiss Confederation at the time, also set out the Federal Council's objectives for 2020. These are coordinated with the three key sets of guiding principles on legislature for the period 2019 to 2023, focusing on «prosperity» (including the further development of the «Digital Switzerland» strategy, the ICT strategy to 2023 and e-government projects), "cohesion" and "security" (covering the management of "cyber-risks", including through a report on how to improve security and prevent misuse in relation to the rapidly growing and scarcely monitored «Internet of Things»).

Documents, declarations of intent, and the will to use digitalisation and secure the provision of relevant services exist to a sufficient extent. However, this must now be followed up promptly by specific actions. In this context, the Advisory Board recommends coordinating and aligning the planned projects in spite of the federal structures and taking the required supporting measures (transparency, public debate, controlled testing, sufficient monitoring and emergency planning) in good time for projects which impact on the security of the population and state.

Challenges

It is important to obtain comprehensive information about the issue at an early stage in order to put forward your own requirements and concerns and to raise any unclear points in depth and in good time during the ongoing debate. Not addressing the issue due to security concerns would be just as ineffective as introducing such services with insufficient reflection and inadequate protection, entailing a correspondingly high risk.

From the perspective of authorities and public administrations etc., particular attention must be paid to constantly maintaining state sovereignty and protecting national interests in an increasingly competitive and globalised economic and political environment.

Provided these requirements are met, there is no reason for concern over existential threats. Failing to take advantage of the opportunities presented by digitalisation for the economy and society would be more harmful long-term than the targeted, controlled assumption of known and manageable risks. However, the challenge is involving all stakeholders in a federal environment to a sufficient extent and developing feasible solutions capable of winning consensus, as well as testing them in a controlled way, improving them where necessary and gradually implementing them.

Need for action

There is an urgent need for action in the following areas, in the order listed below:

– A broad and common understanding of all stakeholder groups in relation to cyber-risks based on risk groups, risk scenarios and their interactions.

– A broad-based discussion and precise definition of the principles and limits of maintaining state sovereignty and “state borders” in the digital world.

– A sufficiently secure, data-protection-compliant, tested and broadly accepted digital identity, and an organisation for natural persons and legal entities that reflects state authority over these identities. This forms the basis for a wide range of e-government services of the Federal Government, the cantons and the municipalities.

– The federally run planning and management of a portfolio of digitalisation projects in authorities and administrations and of corresponding e-government services.

– The definition, testing and management of the required processes for effective, widely accepted interaction between public and private sector actors in the field of digitalisation to create and harness opportunities for Switzerland as a centre of education and business.

– The early identification and compensation or avoidance of unacceptably high dependencies (e.g. from providers controlled by foreign states) and cumulative risks, including adequate emergency and restart planning in the event of problems.

References

– «Digital Switzerland» strategy 2018–20: https://www.bakom.admin.ch/bakom/en/homepage/digital-switzerland-and-internet/strategie-digitale-schweiz.html and https://www.digitalerdialog.ch/en

– National Strategy for Switzerland's Protection against Cyber Risks (NCS): https://www.isb.admin.ch/isb/en/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

Implementation Plan for the National Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018–2022: https://www.newsd.admin.ch/newsd/message/attachments/56943.pdf

Contact

Nicole Wettstein
Head of priority programme Cybersecurity
+41 44 226 50 13

https://www.satw.ch/cybersecurity-challenges

Impressum
Swiss Academy of Engineering Sciences SATW
Expert contributions
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Board of Directors and Advisor | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Editing and graphics
Beatrice Huber, Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020