Information security as a success factor

Secure solutions for the digitization of public authorities

This whitepaper presents the key areas of action within information security and identifies specific approaches to finding solutions.

The challenge of information security

Digitization is an issue of interest and concern to Swiss public authorities and administrations. Besides the opportunities digitization offers, there is a growing awareness of its risks: cyber attacks are a matter of daily concern, while the digital exchange of data is rising sharply.

Studies show that Swiss citizens want to handle their administrative paperwork quickly and easily. Public authorities at all levels of government are responding by continually expanding their e-government services and moving towards "digital first".

However, the expansion of online services also entails additional responsibility because digital government services require high levels of security, and public authorities must provide comprehensive cyber protection.

Decision-makers working in public administration are aware of this responsibility. According to "Trend radar 2022: Approaches for public administration", a study by consulting firm PwC and the University of St. Gallen, 99 percent of people surveyed considered the strengthening of cyber and information security to be "highly relevant".

" Information security is in Swiss Post's DNA. "

Marcel Zumbühl, Chief Information Security Officer at Swiss Post

Digitization requires trust

E-government offers clear advantages: authorities benefit from greater process efficiency, while users get greater flexibility. Yet, there are concerns about data protection.

Generally speaking, the Swiss people have a high level of trust in public authorities when it comes to the handling of confidential data. In the study "Data protection in Switzerland", conducted by Zurich University of Applied Sciences, 74 percent of respondents tended to agree or agreed outright with the statement that public authorities treat personal data properly and confidentially. This high level of approval is a good basis for smoothing out concerns relating to data protection and the use of digital channels.

Data protection governs the right of each individual to determine the use and disclosure of their personal data. The goal of data protection is to protect privacy and prevent misuse of data by third parties. The Federal Act on Data Protection defines how data is collected, processed, used or stored. Information security is critical if all legal requirements concerning data protection in e-government services are to be met. It includes measures and technologies to prevent misuse, falsification and loss of data, and it ensures confidentiality.

Data protection and information security are key elements in further increasing the acceptance of digital solutions and strengthening trust in e-government. This applies both to residents and internally within public authorities. Given the increasing exposure of data to cyber attacks, information security needs to be accorded the highest priority. This creates trust in digital services.

More information on the new FADP:
https://digital-solutions.post.ch/en/data-privacy-incamail

" In terms of cybersecurity, knowing your own risks is key. "

Chief Information Security Officer (CISO) at Swiss Post

5 challenges with regard to information security

Public authorities require secure procedures for the identification, transfer and storage of data to boost their cyber and information security. They currently need to focus on the following five challenges:

1

New Federal Act on Data Protection: more stringent compliance requirements

The new Swiss Federal Act on Data Protection (FADP) comes into force on 1 September 2023, tightening the rules that apply to the processing of personal data.

One of the FADP's key data protection provisions relates to information security. To implement this provision in compliance with the law, an inventory of personal data processing and a risk assessment are needed to determine the requirements for data protection compliance.

Also needed are measures to raise awareness among employees and develop an IT security concept that offers adequate protection against malware and theft or loss of data.

2

Current threat situation: holistic risk management

Cyber attacks are a matter of daily concern. By the time an incident is registered, an average of 100 days have passed. Since the beginning of the year, the National Cyber Security Centre (NCSC) has received 10 000 reports (as at the end of April).

The threat situation has worsened significantly and the methods used by attackers are becoming increasingly sophisticated: according to the NCSC, ransomware as a service (RaaS), supply chain attacks and new social engineering tactics are currently among the most common threats.

The highly dynamic nature of cyberthreats means that holistic risk management is required. Regular hardware and software updates are essential to keep pace with developments.

3

Remote working:
information security while working from home, too
Hybrid forms of work have also taken root in the public authority environment, heightening the risks involved in the processing of sometimes sensitive data. As data becomes more fragmented, the number of vulnerabilities grows. This means solutions are needed to protect data effectively in the home office environment.

4

Building awareness:
training and awareness-raising measures for employees
Technical measures alone do not offer protection against cyber attacks. People need to play a key role in public authority security architectures. After all, employees make a significant contribution to any secure solution. Appreciation of this fact needs to be reinforced with training and awareness-raising campaigns. Preventive measures apply to a wide variety of areas. This may cover handling passwords and access rights. But it also includes familiarity with currently relevant threats. Swift recognition and correct behaviour in connection with a cyber or social engineering attack can prevent considerable damage.

5

Skills shortage:
cybersecurity partners with expertise
The risk of cyber attacks is high. At the same time, there is a shortage of well-trained staff. The security sector does not have enough skilled workers. “We’re fighting for scarce resources in this market,” says Marcel Zumbühl, CISO at Swiss Post. The shortage of skilled people is one of the biggest challenges, which means that having partners with the necessary cyber expertise is important.

Given the growing number of cyber attacks, information security is gaining in importance. **Marcel Zumbühl** explains the measures being implemented by Swiss Post.

Marcel Zumbühl is Chief Information Security Officer (CISO) at Swiss Post.

«Confidential data transport is one of our core competencies – in the digital age too»

Mr Zumbühl, how much of a threat are cyber attacks for Swiss Post?

We register 10 000 viruses per day and 10 million spam e-mails per month. Like all large companies, Swiss Post is a target for cyber criminals. We are actively attacked around 100 times a month.

How does Swiss Post ensure cybersecurity?

We employ about 80 security specialists, out of 1200 IT specialists in total. They are responsible for security monitoring from several cybersecurity centers – around the clock, seven days a week. Our focus here is on participatory security.

What does participatory security mean?

The participatory approach defines security as a chain. This chain is made up of everyone involved – employees, customers and suppliers, who communicate with each other regularly in various communities, mutually strengthening cybersecurity. Another focus is on our "bug bounty".

"Bug bounty" – what's that?

Ethical hackers are given the opportunity to attack us and they receive a financial reward if they report a bug, i.e. a vulnerability, to us. We also routinely simulate artificial attacks and subject our products to around 100 targeted tests every year. What this shows is that cyber-security is an ongoing process. Swiss Post also offers services to public authorities in the protected transfer of sensitive data, such as e-voting.

Why is Swiss Post a trustworthy partner?

The confidential and secure transport of sensitive data is part of Swiss Post's DNA – and that remains the case in the digital age. We offer our customers transparency. In e-voting, for example, we published the code for down-load, enabling the aforementioned "part-icipatory security" that allows for continuous improvement of the system. The e-voting system also guarantees data protection with state-of-the-art cryptographic procedures.

Which security issues of the future are you currently concerned with?

Today we protect data, tomorrow algorithms. So we're looking very closely at how artificial intelligence can be protected. We're also getting ready for quantum computers, which will be able to break encryption methods very much faster than conventional comput-ers. And thirdly, we're conducting research in relation to the smart city. As Switzerland's second largest passenger transport company, we naturally want to be ready when means of transport such as postbuses can be networked with the infrastructure.

Measures to strengthen cybersecurity

Fundamental issues of security always need to be considered in digitization projects. Along with Swisscom, Microsoft and other companies, Swiss Post is a sponsor of Swiss Cyber Defence DNA, which in its guidelines recommends six measures at the organisational and technological levels:

1 Up-to-date unchangeable data backup / write-protected backup

- Define a person for implementation and review
- Ensure external storage of the backup

- Automated, write-protected backup process including encryption
- If the above is not possible: disconnect the backup medium from the network and store it offline

2 Comprehensive and up-to-date protection against malware

- Awareness-raising and training of employees with regard to dealing with e-mails, websites, passwords etc.

- Comprehensive, companywide malware protection for end devices, servers, cloud and e-mail services
- Restrict macro execution; install internet and spam filters

3 Harden networks and remote access

- Training of employees and suppliers for remote access

- Use a firewall to divide your network into zones so that important business areas are segregated
- Additionally secure remote access using 2-factor authentication (e.g. SMS code)

4 Keep hardware and software up to date

- Define a person who is responsible for the administration and periodic review of the licenses/updates

- According to the risk assessment, replace outdated systems and physically protect existing ones (e.g. access to the server)
- Use only current operating systems and applications

5 Employees and their roles

- Use a role concept to define which rights are necessary for each employee
- Also check and restrict management access rights

- Create password rules for employees
- Link and restrict defined roles with the access rights

6 Define emergency processes

- Determine the emergency organization, define processes and inform all employees
- Regularly review roles and processes and restore data frequently

- Use independent technology to ensure documents can be accessed even in an emergency (e.g. emergency note, paper folder, cloud or mobile solution)

Information security needs trustworthy partners

Swiss authorities and public administrations are pushing ahead with the digitization of their services. One success factor in this process is information security, which constitutes the basis for the trustworthy exchange of data between residents and public authorities.

If e-government services are to be widely used, they need to be simple and secure. This is achieved by focusing consistently on the requirements of their users.

This includes:

Data sovereignty: Residents know what data is collected and stored, who uses and processes it.

Information security: Thanks to secure authentication, only authorized persons can access personal data. Secure channels are available to the public and authorities for the exchange of data.

Cybersecurity: Facilities and systems operated by authorities are protected against attacks with serious consequences and are regularly monitored for cyberattacks.

Digital empowerment: Services are intuitive enough to allow anyone to use them or easily learn the skills needed to do so.

Swiss Post as a partner

Trust is a key factor in the success of e-government projects. Thanks to its network, Swiss Post is a trustworthy partner. Whether it's for handling individual processes digitally, protecting the entire digital infrastructure or exchanging sensitive data – we offer secure, simple and pragmatic solutions. We're committed to digitization that takes everyone on board thanks to intuitive online services and front-line staff who bridge the gap between digital and analogue.

Find out more
E-Government | Swiss Post

Up to speed at all times
Swiss Post | E-Government: Posts | LinkedIn