Information security at Swiss Post

Simply a good feeling

Foreword

Marcel Zumbühl
CISO, Swiss Post

Dear Customer

Information security is far more than a technology issue. That's because the best technology doesn't help if there is no trust in it. Swiss Post believes it is very important to give you this feeling of confidence and to advise and assist you with all your information security-related questions.

The security of your data is of central importance to us. This begins right from the time we develop a solution, long before you can use our products and services as a customer. And we of course ensure that your data is and remains appropriately secure during ongoing operations. For instance, we subject our products to regular testing and monitor operations in our data centers around the clock. This means we can identify attacks by hackers at an early stage and take countermeasures.

We also regularly scrutinize ourselves, in partnership with renowned external experts. By doing so, we can identify how and where we need to improve security for our customers. Standing still is not an option when it comes to security. Proof of the high quality of information security management that Swiss Post provides comes from the independent auditors who examine and document our measures annually in accordance with international security standards.

All of these security measures are undertaken in the background simply as a matter of course. And they have just one goal, namely for our products and services to be able to contribute to your success through their seamless and reliable operations, and for you to feel completely safe and secure when using them.

Kind regards
Marcel Zumbühl, CISO, Swiss Post

Information security at Swiss Post

This folder contains various factsheets about the information security of our main products and services. The information published here is reviewed and updated on an ongoing basis. This is undertaken as part of a close partnership between Product Management, Security Officers, Communication and Swiss Post's Legal Service. If you have further questions, please contact your customer advisor or Swiss Post's Information Security unit.

Information security – most common threats and countermeasures

Information is valuable. That's why it needs to be protected from criminal attackers. These individuals attempt to exploit vulnerabilities to gain illegal benefits. Common attacks include theft of information, phishing and identity misuse, the destruction and manipulation of information and denial of service attacks against data centers.

Theft of information

Procedure: Criminals break into computer systems, steal information and sell this on the black market. Favoured targets of attackers include personal information, corporate data, credit card details and general information about financial processes. Criminals often use false identities to trick their way into gaining the victim's trust and to get access to what they need.

Assessment: This pattern of attacks is incredibly widespread. It requires a high level of technical knowledge or the appropriate professional tools. Moreover, the attacker needs to have access to a network of receivers, in order to be able to sell the data.

Countermeasures: Systems in Swiss Post's data centers are guarded by several layers of protection and are under permanent surveillance. Vulnerabilities are continuously being sought, in order to eliminate them or to limit them by taking additional measures.

Phishing and identity theft

Procedure: Criminals trick their way into gaining the trust of the victim by using fake e-mails, text messages or even phone calls, and assume that individual's digital identity. They can also purchase identities of victims (e.g. account access) on the black market. Using the stolen identity, they attempt to order goods, manipulate services or to immediately plunder bank accounts.

Assessment: Widespread and does not require major technical capabilities from the attacker. This type of attack normally comes in waves.

Countermeasures: Combating identity theft and phishing successfully requires great vigilance and a speedy response both from customers and Swiss Post. Attacks can be identified and blocked based on slight deviations in text and language or in the behaviour of systems.

Data manipulation and information loss

Procedure: Criminals penetrate systems, create a copy of information and destroy the original one or encrypt it in such a way that it is no longer accessible. Subsequently, they blackmail the victim by using the stolen information or the access tools to hold them to ransom.

Assessment: Attacks are usually carried out on a targeted basis. They require deep technical knowledge as well as detailed knowledge about the victim.

Countermeasures: Swiss Post uses a range of protective measures to ward off these kinds of attacks. It also works closely with law enforcement authorities. This means that it can react decisively when an attack is attempted.

Denial of service attacks against infrastructure

Procedure: Criminals launch targeted attacks against services until these are overwhelmed and can no longer be accessed online. Subsequently, the perpetrators blackmail the victim and demand money to end the denial of service situation.

Assessment: Attacks are undertaken sporadically, mainly in the form of exploratory attempts to test the strength of the protective mechanisms. The attacks require deep technical knowledge and dedicated, high-performance infrastructure.

Countermeasures: Swiss Post works together with Internet providers to ensure that it has defence mechanisms that are reviewed regularly, in order to defend itself against denial of service attacks.

Additional ways to protect yourself

The most important rules for more security:
- Use strong passwords
- Carry out updates regularly
- Protect your network and Internet connection
- Encrypt your data
- Be cautious when dealing with dubious e-mails and enquiries

You can also find current information about information security on the official websites of specialized organizations. We can recommend the following to you:

- National Cyber Security Centre, or NCSC (previously known as MELANI) – www.ncsc.admin.ch
- Swiss Cyber Experts – www.swiss-cyber-experts.ch
- ICT Switzerland – www.ictswitzerland.ch
- ebas.ch – www.ebas.ch

Data protection

As a service provider to its customers, Swiss Post believes that managing personal data in a responsible, legally-compliant manner is very important.

To this end, Swiss Post ensures that data is handled responsibly and in compliance with the applicable statutory data protection provisions and postal legislation.

Swiss Post has a comprehensive data protection management system and verifies that all its services comply with data protection provisions.

Certified security

For key issues, Swiss Post seeks certification in accordance with internationally recognized standards. By doing so, it adheres to best practices and simplifies compliance processes for customers. The certification process includes the following standards.

ISO 27001
The international standard specifies the requirements for the installation, implementation, maintenance and ongoing improvements for an information security management system (ISMS).

ISO 22301
The international standard specifies the requirements for creating and operating an effective Business Continuity Management System (BCMS).

TÜV Trusted Site Infrastructure TSI V3.2 Dual Site Level 3
Both of Swiss Post's data centers are located in Switzerland, in different geographical locations. They provide a first-class hosting environment with several layers of security. The standard defines specifications for the physical infrastructure of a data center (location, building construction, security technology, energy supply and air conditioning technology) and the operator's organizational processes. The standard also documents the suitability of secure areas for which a high level of availability is required.

ISAE 3402
PostFinance (as a financial institution) and Swiss Post Solutions (as a service provider for financial institutions), along with Swiss Post Informatics, are assessed and certified in accordance with the International Standard on Assurance Engagements (ISAE) 3402 for control effectiveness of the internal control system.

PCI DSS
The Payment Card Industry Data Security Standard (PCI DSS) was developed by the PCI Security Standards Council to combat scams relating to credit card payments on the Internet.

Postshop
Shop securely in Swiss Post's online shop

At postshop.ch, you can order a wide range of products to make your everyday life easier with the click of a mouse. Security when shopping is guaranteed thanks to the encryption of information and a certified payment platform.

Various access options

Those wanting to make purchases from the Postshop can either log in using their Swiss Post Customer Login or SwissID, or order as a guest. However, only registered customers can pay by invoice and redeem vouchers. In addition, gift cards and e-vouchers cannot be purchased by invoice. These measures make it more difficult for any attempts at fraud to succeed.

High availability

In the first half of 2020, the Postshop was available 99.5 percent of the time. To ensure that the site is able to cope with large volumes, Swiss Post regularly conducts stress tests. It also actively monitors availability and checks whether the specified benchmarks are upheld.

Secure payment system

Postshop customer data is storedsolely in Switzerland. Customers paying by credit card are transferred from Postshop to Billing-Online, Swiss Post's secure and PCI DSS-certified payment platform. This global security standard protects relevant data from cyber theft and fraudulent use. All network traffic via the Internet is encrypted.

Extensive tests

Swiss Post reviews and optimizes its Postshop on an ongoing basis. Postshop participates in Swiss Post's bug bounty programme. This means that any identified vulnerabilities (findings) can be immediately rectified. Swiss Post also regularly subjects its computers and networks to a comprehensive security test that is based on international standards (OWASP Top 10).
Swiss Post also periodically analyses protection requirements and its information security plan. Security tests are conducted by an independent checking department before each major update to Postshop.

What is Postshop?
Postshop is Swiss Post's online shop. It offers goods and services that are related to Swiss Post's business, from smartphones to gift cards and travel accessories. The latest stamps from Swiss Post and suitable packaging material for sending letters and parcels can also conveniently be ordered at the click of a mouse.
www.postshop.ch

2020-072 (InfoSec) 05.2021

Post CH Ltd
Wankdorfallee 4
3030 Bern
Switzerland

Tel. +41 848 888 888
E-mail post@swisspost.ch
www.swisspost.ch

SWISS POST

Delivery services
Convenient and secure

With its delivery services, Swiss Post offers a wide range of options for managing incoming mail with ease, whether you're a private customer or business customer.

Personal identification

Swiss Post's delivery services are available to all customers. Business customers also need to present proof of their status, such as a commercial register excerpt or articles of association. Swiss Post only confirms that it has seen the identification documents. It does not keep the documents themselves and it does not store them.

Fully-automated data flow

The data collected as part of these services is automatically passed on to a central application at Swiss Post. This ensures that all relevant services always have access to the latest data. The data remains in Swiss Post's possession at all times.

Strictly regulated access

Only Swiss Post employees with specific user rights have access to the delivery services or the central application that stores the data required for the services. If a user is inactive for 90 days, his or her access will automatically be deleted.

Protecting themselves

Customers can give themselves additional protection by selecting as strong a password as possible for their Swiss Post Customer Login and neither storing this in the browser, nor sharing it with others.

What are delivery services?
Creating and managing forwarding orders, changing addresses and reporting moves – these are just some of the many delivery services that Swiss Post offers its customers. They can be accessed online around the clock (from PCs, smartphones and tablets) using a Swiss Post Customer Login or at the counter during opening hours or via Customer Service.
www.swisspost.ch/receiving-mail

2020-072 (InfoSec) 05.2021

Post CH Ltd
Wankdorfallee 4
3030 Bern
Switzerland

Tel. +41 848 888 888
E-mail post@swisspost.ch
www.swisspost.ch

SWISS POST

PubliBike
Secure while on the go

PubliBike can be used to hire bicycles and e-bikes throughout Switzerland. To register, a Swiss Post Customer Login is needed. Billing is made on a per-minute basis, with payment being made by credit card. Swiss Post ensures that the service is secure and remains that way.

Redundancy ensures availability

PubliBike data is stored in two data centers that are certified under ISO 27001. If one data center suffers an outage, the redundancy ensures that the data and PubliBike operations are secured. Customer interactions take place via different servers. This avoids overloading any one particular server.

Secure handling of data

Protection of your personal data is of great importance to us. We therefore handle your personal data with great care and in compliance with the applicable statutory data protection provisions and further legal principles. All data traffic via the Internet is encrypted.

Security measures

An attack detection system is used to immediately recognize, investigate and prevent unauthorized changes to PubliBike systems. The systems are also regularly monitored to identify vulnerabilities, including with a comprehensive security test that is based on international standards (OWASP Top 10). The use of system components is recorded in a logbook to allow follow up, with irregularities being investigated

What is PubliBike?
PubliBike is the largest bike sharing service in Switzerland. It is the ideal complement to public and private transport over short distances, easing traffic congestion in city centers while improving users' health. PubliBike is also suitable for connecting business locations, such as universities, administrations or large company premises. www.publibike.ch

2020-072 (InfoSec) 05.2021

Post CH Ltd
Wankdorfallee 4
3030 Bern
Switzerland

Tel. +41 848 888 888
E-mail post@swisspost.ch
www.swisspost.ch

SWISS POST

Document Input Processing
Scan and prepare documents securely

Swiss Post Solutions uses Document Input Processing (DIP) to process unstructured data from incoming physical and electronic documents for its business customers. Data protection is ensured throughout this process.

High availability

Swiss Post Solutions (SPS) takes various measures to ensure the highest level of service availability. These include, for example, mirrored data center infrastructure, regular recovery tests and database backups, as well as a redundant network connection for the locations with what are known as 'fail-over' mechanisms. These ensure that a second machine seamlessly assumes the tasks of the first if a server breaks down.

End-to-end encryption

With Document Input Processing (DIP), the exchange of data with customers is always undertaken on an encrypted basis, using the Secure File Transfer Protocol (SFTP) and/or a Virtual Private Network (VPN) tunnel. The network zones are also protected with firewalls.

Technical security measures

Within SPS's protected network, DIP runs via a dedicated Virtual Local Area Network (VLAN). The VLAN can be accessed only via multi-factor authentication. Log monitoring is used to analyse log files in real time and to trace all transactions. Thanks to active network monitoring, potential cyber attacks are identified and thwarted at an early stage.

Physical security measures

Only SPS staff with a special badge have access to the DIP production rooms. Staff are subject to a duty of confidentiality and postal secrecy. Access to the facilities is logged and the building is under video surveillance. Before receiving expanded user rights, staff are also assessed in a screening procedure.

International security standards

Extensive security guidelines apply to DIP, such as ISO standard 27001 for information security, the Payment Card Industry Data Security Standard (PCI DSS) for credit card transactions (in Switzerland) and the Health Insurance Portability and Accountability Act (HIPAA) for the protection of healthcare information (in the USA). Compliance with these standards is verified regularly.

What is Document Input Processing?
Swiss Post Solutions uses Document Input Processing (DIP) to optimize document-based business processes. The processing operations are highly standardized and are systematically developed and enhanced. From the acceptance and preparation of documents, to scanning, indexing and processing, through to archiving, DIP offers all the steps needed for the automatic preparation of unstructured data and for its provision to customers.
www.swisspostsolutions.com/dip

2020-072 (InfoSec) 05.2021

Post CH Ltd
Wankdorfallee 4
3030 Bern
Switzerland

Tel. +41 848 888 888
E-mail post@swisspost.ch
www.swisspost.ch

SWISS POST

Document Output Processing
Secure output management for business customers

For its business customers, Swiss Post Solutions uses Document Output Processing for data preparation, printing and to send their transaction-related documents. Data protection is ensured throughout this process.

High availability

Document Output Processing (DOP) from Swiss Post Solutions (SPS) operates production sites at major letter centers for data preparation, printing and the dispatch of documents. Along with various back-up and recovery procedures, there is also an emergency operations mode in the production sites to ensure availability during an extraordinary event.

End-to-end encryption

When DOP is used, data is exchanged in encrypted form via the Secure File Transfer Protocol (SFTP) and/or a Virtual Private Network (VPN) tunnel. The network zones are also protected with firewalls.

Technical security measures

Within SPS's protected network, DOP runs via a dedicated Virtual Local Area Network (VLAN). The VLAN can be accessed only via multi-factor authentication. A full system of log monitoring is used to analyse the log files. Moreover, all transactions are traceable and are stored in an unimpeachable manner. External certified partners ensure that a standardized destruction process for storage media is followed.

Physical security measures

Only SPS staff with a special badge have access to DOP's production rooms. Staff are subject to a duty of confidentiality and postalsecrecy. Access to the facilities is logged and the building is under video surveillance. Before receiving expanded user rights, staff are also assessed in a screening procedure.

International security standards

Extensive security guidelines apply to DOP, such as ISO standard 27001 for information security, the Payment Card Industry Data Security Standard (PCI DSS) for credit card transactions (in Switzerland) and the Health Insurance Portability and Accountability Act (HIPAA) for the protection of healthcare information (in the USA). Compliance with these standards is verified regularly.

What is Document Output Processing?
Swiss Post Solutions uses Document Output Processing for its business customers to print and deliver transaction-based business documents such as invoices, insurance policies and account statements. The documents can be transmitted to the end customer in physical or digital form, or in a mix of both.The automation of output management conserves resources, while simultaneously guaranteeing stability, security and economic viability.
www.swisspostsolutions.com/dop

2020-072 (InfoSec) 05.2021

Post CH Ltd
Wankdorfallee 4
3030 Bern
Switzerland

Tel. +41 848 888 888
E-mail post@swisspost.ch
www.swisspost.ch

SWISS POST

2020-072 (InfoSec) 05.2021

Post CH Ltd
Wankdorfallee 4
3030 Bern
Switzerland

Tel. +41 848 888 888
E-mail post@swisspost.ch
www.swisspost.ch

SWISS POST