Informationssicherheit bei der Schweizerischen Post

Einfach ein gutes Gefühl

Vorwort

Marcel Zumbühl
CISO, die Schweizerische Post

Sehr geehrte Kundin, sehr geehrter Kunde

Informationssicherheit ist weit mehr als eine Frage der Technik. Denn die beste Technik nützt nichts, wenn eines fehlt: das Vertrauen in sie. Der Schweizerischen Post ist es ein grosses Anliegen, Ihnen dieses Vertrauen zu vermitteln und Sie bei all Ihren Fragen rund um das Thema Informationssicherheit zu beraten und zu unterstützen.

Die Sicherheit Ihrer Daten ist für uns zentral. Das beginnt schon bei der Entwicklung eines Angebots, also schon lange bevor Sie als Kundin oder Kunde unsere Dienstleistungen und Produkte nutzen können. Und natürlich sorgen wir während des laufenden Betriebs dafür, dass Ihre Daten angemessen sicher sind und sicher bleiben. Beispielsweise, indem wir unsere Produkte regelmässigen Tests unterziehen und den Betrieb rund um die Uhr in unseren Rechenzentren überwachen. Dadurch können wir Angriffsversuche von Hackern früh erkennen und Gegenmassnahmen ergreifen.

Darüber hinaus stellen wir uns auch regelmässig in Zusammenarbeit mit renommierten externen Expertinnen und Experten auf die Probe. So erkennen wir, wie und wo wir die Sicherheit für unsere Kundinnen und Kunden weiter verbessern können. Stillstand gibt es in der Sicherheit nicht. Die hohe Qualität, mit der die Post die Informationssicherheit managt, bestätigen unabhängige Zertifiktatoren, die unsere Massnahmen jährlich nach internationalen Sicherheitsstandards untersuchen und dokumentieren.

All diese Sicherheitsmassnahmen erfolgen ganz selbstverständlich im Hintergrund. Und sie haben nur ein Ziel: dass wir mit einem reibungslosen und zuverlässigen Betrieb unserer Produkte und Dienstleistungen zu Ihrem Erfolg beitragen dürfen und Sie sich dabei rundum sicher fühlen.

Herzlich,
Marcel Zumbühl, CISO, die Schweizerische Post

Informationssicherheit bei der Post

Diese Mappe enthält verschiedene Factsheets rund um die Informationssicherheit unserer Hauptprodukte und Dienstleistungen. Die hier publizierten Informationen werden laufend überprüft und angepasst. Dies geschieht in enger Zusammenarbeit zwischen dem Produktmanagement, den Sicherheitsverantwortlichen, der Kommunikation und dem Rechtsdienst der Schweizerischen Post. Wenn Sie weiterführende Fragen haben, wenden Sie sich bitte an Ihre Kundenberaterin, Ihren Kundenberater oder an die Informationssicherheit der Post.

Informationssicherheit – häufigste Bedrohungen und Gegenmassnahmen

Informationen sind wertvoll. Deshalb müssen sie vor kriminellen Angreifern geschützt werden. Diese versuchen, Schwachstellen auszunutzen, um sich unrechtmässige Vorteile zu verschaffen. Die gängigen Angriffe sind dabei der Diebstahl von Informationen, Phishing und Missbrauch von Identitäten, die Zerstörung und Manipulation von Informationen sowie Überlastangriffe gegen Rechenzentren.

Diebstahl von Informationen

Vorgehen: Kriminelle brechen in Computersysteme ein, entwenden Informationen und verkaufen diese auf dem Schwarzmarkt. Beliebte Ziele von Angreifern sind persönliche Informationen, Unternehmensdaten, Kreditkartendaten und generell Informationen rund um finanzielle Prozesse. Oftmals versuchen Kriminelle unter Vorgabe falscher Identitäten, das Vertrauen des Opfers zu erschleichen, um so an die richtige Stelle zu gelangen.

Einschätzung: Dieses Angriffsmuster ist mässig verbreitet. Es setzt hohe technische Kenntnisse oder die entsprechenden professionellen Werkzeuge voraus. Darüber hinaus muss der Angreifer Zugang zu einem Hehlernetzwerk verfügen, um die Daten verkaufen zu können.

Gegenmassnahmen: Systeme in den Rechenzentren der Post sind durch mehrere Schutzebenen geschützt und stehen unter permanenter Überwachung. Kontinuierlich wird nach Schwachstellen gesucht, um diese zu beheben oder mit zusätzlichen Massnahmen einzuschränken.

Phishing und Identitätsdiebstahl

Vorgehen: Kriminelle erschleichen sich das Vertrauen des Opfers durch gefälschte E-Mails, Textnachrichten oder sogar Anrufe und übernehmen die digitale Identität des Opfers. Sie können sich auch Identitäten von Opfern (z. B. Kontenzugriffe) auf dem Schwarzmarkt erkaufen. Mithilfe der ergaunerten Identität versuchen sie, Waren zu bestellen, Dienstleistungen zu manipulieren oder direkt Bankkonten auszurauben.

Einschätzung: weitverbreitet und setzt keine grossen technischen Fähigkeiten seitens Angreifer voraus. Meist erfolgt diese Angriffsart in Wellen.

Gegenmassnahmen: Die erfolgreiche Bekämpfung von Identitätsdiebstählen und Phishing setzt sowohl bei Kundinnen und Kunden als auch auf Seite der Post grosse Wachsamkeit und rasche Reaktionen voraus. Angriffe können anhand von geringfügigen Abweichungen in Text und Sprache oder im Verhalten von Systemen entdeckt und blockiert werden.

Datenmanipulation und Informationsverlust

Vorgehen: Kriminelle dringen in Systeme ein, erstellen eine Kopie von Informationen und zerstören das Original oder verschlüsseln es, sodass es nicht mehr zugänglich ist. Anschliessend erpressen sie das Opfer, indem sie die erbeutete Information oder die Zugangsmittel zu den Daten als Pfand nutzen.

Einschätzung: Angriffe werden meist gezielt durchgeführt. Sie erfordern tiefes technisches Wissen sowie detaillierte Kenntnisse über das Opfer.

Gegenmassnahmen: Zur Abwehr solcher Angriffe setzt die Post eine Vielzahl von Schutzmechanismen ein. Sie arbeitet auch eng mit Strafverfolgungsbehörden zusammen. So kann sie schon auf den Versuch einer Attacke entschieden reagieren.

Überlastangriffe gegen Infrastrukturen

Vorgehen: Kriminelle attackieren gezielt den Zugriff auf Dienstleistungen, bis dieser überlastet und aus dem Internet nicht mehr zu erreichen ist. Anschliessend erpressen sie das Opfer und fordern für die Aufhebung der Überlastsituation Geld.

Einschätzung: Angriffe erfolgen sporadisch, meist in Form von Abtastversuchen, um die Stärke der Schutzmechanismen zu testen. Die Attacken setzen tiefe technische Kenntnisse und eine dedizierte performante Infrastruktur voraus.

Gegenmassnahmen: Die Post verfügt in Zusammenarbeit mit Netzanbietern über regelmässig geprüfte Abwehrmechanismen, um Überlastangriffe abwehren zu können.

So können Sie sich zusätzlich schützen

Die wichtigsten Regeln für mehr Sicherheit:
- Verwenden Sie starke Passwörter
- Führen Sie regelmässig Updates durch
- Schützen Sie Ihre Netzwerk- und Internetverbindung
- Verschlüsseln Sie Ihre Daten
- Lassen Sie bei dubiosen E-Mails und Anfragen Vorsicht walten

Aktuelle Informationen rund um Informationssicherheit finden Sie auch auf den offiziellen Websites spezialisierter Organisationen. Folgende können wir Ihnen empfehlen:

- Nationales Zentrum für Cybersicherheit NSCS (früher MELANI) – www.ncsc.admin.ch
- Swiss Cyber Experts – www.swiss-cyber-experts.ch
- ICT Switzerland – www.ictswitzerland.ch
- ebas.ch – www.ebas.ch

Datenschutz

Im Rahmen der Leistungserbringung gegenüber ihren Kunden ist der Post der verantwortungsvolle und rechtskonforme Umgang mit Personendaten ein grosses Anliegen.

Die Post stellt dabei sicher, dass die Daten mit grosser Sorgfalt und gemäss den einschlägigen gesetzlichen Bestimmungen des Datenschutzrechts sowie der Postgesetzgebung behandelt werden.

Die Post verfügt über ein umfassendes Datenschutzmanagementsystem und prüft jede Dienstleistung auf ihre Datenschutzkonformität.

Zertifizierte Sicherheit

Die Schweizerische Post lässt sich in Schlüsselthemen auf international anerkannte Standards zertifizieren. Damit hält sie sich an die Best Practices und vereinfacht die Compliance-Prozesse der Kunden. Unter anderem sind dies die folgenden Standards.

ISO 27001
Die internationale Norm spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheits-Managementsystems (ISMS).

ISO 22301
Die internationale Norm spezifiziert die Anforderungen für die Erstellung und den Umgang mit einem effektiven Business Continuity Management System (BCMS).

TÜV Trusted Site Infrastructure TSI V3.2 Dual Site Level 3
Beide Rechenzentren der Post befinden sich in der Schweiz und an geografisch unabhängigen Standorten. Sie bieten eine erstklassige Hosting-Umgebung mit mehreren Sicherheitsebenen. Das Zertifikat definiert Anforderungen an die physische Infrastruktur eines Rechenzentrums (Standort, Baukonstruktion, Sicherheitstechnik, Energieversorgung und Kältetechnik) und die organisatorischen Prozesse des Betreibers. Zudem dokumentiert es die Eignung für Sicherheitsbereiche, für die eine hohe Verfügbarkeit verlangt wird.

ISAE 3402
PostFinance als Finanzinstitut und Swiss Post Solutions als Service Provider für Finanzinstitute werden zusammen mit der Post Informatik nach dem International Standard on Assurance Engagements (ISAE) 3402 auf die Kontrollwirksamkeit des internen Kontrollsystems geprüft und zertifiziert.

PCI DSS
Der Payment Card Industry Data Security Standard (PCI DSS) wurde vom PCI Security Standards Council entwickelt, um Betrügereien bei Kreditkartenzahlungen im Internet einzudämmen.

Postshop
Sicher einkaufen im Webshop der Post

Auf postshop.ch können viele Angebote, die den Alltag leichter zu machen, per Mausklick bestellt werden. Garantiert wird die Sicherheit beim Einkauf durch die Verschlüsselung von Informationen und eine zertifizierte Zahlungsplattform.

Verschiedene Zugriffsmöglichkeiten

Wer im Postshop einkaufen möchte, kann sich entweder via Kundenlogin Post oder mit SwissID anmelden oder aber als Gast bestellen. Auf Rechnung bezahlen und Gutscheine einlösen können jedoch nur registrierte Kunden. Zudem lassen sich Geschenkkarten und E-Gutscheine nicht auf Rechnung kaufen. Diese Massnahmen erhöhen die Hürde für allfällige Betrugsversuche.

Hohe Verfügbarkeit

Im ersten Halbjahr 2020 war der Postshop zu 99,5 Prozent verfügbar. Um auch auf grosse Volumen reagieren zu können, führt die Post periodisch Lastentests durch. Ausserdem wertet sie durch aktives Monitoring die Verfügbarkeit aus und prüft, ob die definierten Benchmarks eingehalten werden.

Sicheres Zahlsystem

Die Daten der Postshop-Kunden werden ausschliesslich in der Schweiz gespeichert. Wer mit Kreditkarte bezahlt, wird vom Postshop weitergeleitet auf BillingOnline, die sichere und PCI-DSS-zertifizierte Zahlungsplattform der Post. Dieser globale Sicherheitsstandard schützt die betreffenden Daten vor Cyber-Diebstahl und betrügerischer Nutzung. Jeglicher Netzwerkverkehr über das Internet erfolgt verschlüsselt.

Umfassende Tests

Die Post überprüft und optimiert ihren Postshop laufend. Einerseits ist der Postshop im Bug-Bounty-Programm der Post vertreten. Das heisst, dass allfällig identifizierte Schwachstellen (Findings) umgehend korrigiert werden können. Andererseits unterzieht die Post ihre Rechner und Netzwerke regelmässig einem umfassenden Sicherheitstest, der sich an internationalen Standards (OWASP Top 10) orientiert. Zudem analysiert die Post periodisch den Schutzbedarf und das Konzept zur Informationssicherheit und lässt vor jedem grossen Update des Postshops von einer unabhängigen Prüfstelle Sicherheitstests durchführen.

Was ist Postshop?
Postshop ist der Onlineshop der Post. Er bietet Waren und Dienste an, die einen Bezug zum Geschäft der Post aufweisen: von Smartphones über Geschenkkarten bis zu Reisezubehör. Auch die neuesten Briefmarken der Post sowie passendes Verpackungsmaterial für den Versand von Briefen und Paketen können bequem per Mausklick bestellt werden.
www.postshop.ch

2020-072 (InfoSec) 05.2021

Post CH AG
Wankdorfallee 4
3030 Bern

Telefon 0848 888 888
E-Mail post@post.ch
www.post.ch

DIE POST

Zustelldienstleistungen
Praktisch und sicher

Ob für Privat- oder Geschäftskunden: Die Post bietet mit ihren Zustelldienstleistungen zahlreiche Möglichkeiten, den Postempfang bequem zu steuern.

Persönliche Identifizierung

Die Zustelldienstleistungen der Post stehen allen Kundinnen und Kunden zur Verfügung. Für die Nutzung ist eine persönliche Identifizierung zwingend. Geschäftskunden müssen zusätzlich einen Beleg vorweisen, beispielsweise einen HR-Auszug oder Vereinsstatuten. Die Post bestätigt nur, dass sie die Identifizierungsdokumente gesehen hat. Die Dokumente selbst behält sie nicht und speichert sie auch nicht ab.

Vollautomatisierter Datenfluss

Die im Rahmen dieser Dienstleistungen erhobenen Daten werden über eine zentrale Applikation bei der Post vollständig automatisiert weitergeleitet. So ist sichergestellt, dass alle betroffenen Dienste immer über die aktuellen Daten verfügen. Die Daten bleiben jederzeit bei der Post.

Strikt geregelter Zugriff

Zu den Zustelldienstleistungen bzw. der zentralen Applikation, die die für die Services erforderlichen Daten speichert, haben nur Postmitarbeitende mit spezifischen Benutzerrechten Zugriff. Ist ein Benutzer während 90 Tagen inaktiv, wird seine Berechtigung automatisch gelöscht.

Sich selbst schützen

Kundinnen und Kunden können sich selbst zusätzlich schützen, indem sie für das Kundenlogin Post ein möglichst starkes Passwort wählen und dieses weder im Browser speichern noch mit anderen teilen.

Was sind Zustelldienstleistungen?
Nachsendeaufträge eröffnen und verwalten, Adressen ändern und Umzüge melden – dies sind nur einige der zahlreichen Zustelldienstleistungen, die die Post ihren Kundinnen und Kunden anbietet. Nutzen lassen sie sich rund um die Uhr online (PC, Smartphone, Tablet) über das Kundenlogin Post oder während der jeweiligen Öffnungszeiten am Postschalter beziehungsweise über den Kundendienst.
www.post.ch/empfangen

2020-072 (InfoSec) 05.2021

Post CH AG
Wankdorfallee 4
3030 Bern

Telefon 0848 888 888
E-Mail post@post.ch
www.post.ch

DIE POST

PubliBike
Sicher unterwegs

Mit PubliBike lassen sich schweizweit Velos und E-Bikes ausleihen. Für die Anmeldung braucht es ein Login, die Verrechnung erfolgt auf Minutenbasis, bezahlt wird via Kreditkarte. Die Post sorgt dafür, dass der Dienst sicher ist und sicher bleibt.

Redundanz sichert Verfügbarkeit

Die Daten von PubliBike werden in zwei ISO-27001-zertifizierten Rechenzentren gespeichert. Sollte ein Rechenzentrum ausfallen, ist dank Redundanz garantiert, dass die Daten und der Betrieb von PubliBike gesichert sind. Kundeninteraktionen erfolgen über verschiedene Server. So lässt sich eine zu hohe Auslastung eines einzelnen Servers vermeiden.

Vertraulicher Umgang mit Daten

Der Schutz der persönlichen Daten liegt der Post sehr am Herzen. Daher behandelt sie persönliche Daten mit grosser Sorgfalt und gemäss den einschlägigen gesetzlichen Bestimmungen des Datenschutzrechts sowie weiterer gesetzlicher Grundlagen. Der gesamte Datenvekehr über das Internet erfolgt veschlüsselt.

Sicherheitsmassnahmen

Mithilfe eines Angriffserkennungssystems werden unberechtigte Veränderungen an den Systemen von PubliBike sofort erkannt, untersucht und unterbunden. Zudem werden die Systeme regelmässig auf Schwachstellen überprüft, unter anderem mit einem umfassenden Sicherheitstest, der sich an internationalen Standards (OWASP Top 10) orientiert. Die Nutzung der Systemkomponenten wird in einem Logbuch zur Nachverfolgung aufgezeichnet und auf Irregularitäten überprüft.

Was ist PubliBike?
PubliBike ist das schweizweit grösste Bikesharing-Angebot. Es ist die ideale Ergänzung zu privaten und öffentlichen Verkehrsmitteln im Kurzstreckenbereich, entschärft die Verkehrsbelastung in den Innenstädten und fördert die Gesundheit der Nutzerinnen und Nutzer. PubliBike eignet sich auch zur Vernetzung von Firmenstandorten, zum Beispiel von Universitäten, Verwaltungen oder grossen Firmengeländen.
www.publibike.ch

2020-072 (InfoSec) 05.2021

Post CH AG
Wankdorfallee 4
3030 Bern

Telefon 0848 888 888
E-Mail post@post.ch
www.post.ch

DIE POST

Document Input Processing
Dokumente sicher scannen und aufbereiten

Mit Document Input Processing (DIP) verarbeitet Swiss Post Solutions für ihre Geschäftskunden unstrukturierte Daten aus eingehenden physischen und elektronischen Dokumenten. Der Datenschutz ist dabei sichergestellt.

Hohe Verfügbarkeit

Mit verschiedenen Massnahmen sorgt Swiss Post Solutions (SPS) für höchste Serviceverfügbarkeit. Dazu gehören beispielsweise eine gespiegelte Rechenzentrum-Infrastruktur, regelmässige Wiederherstellungstests und Datenbanksicherungen sowie eine redundante Netzwerkanbindung der Standorte mit sogenannten Fail-over-Mechanismen. Diese gewährleisten, dass bei einem Rechnerausfall der zweite Rechner nahtlos die Aufgaben des ersten übernimmt.

End-to-End-Verschlüsselung

Der Datenaustausch mit den Kundinnen und Kunden erfolgt beim Document Input Processing (DIP) stets verschlüsselt über ein Secure File Transfer Protocol (SFTP) und/oder Virtual Private Network (VPN) Tunnel. Die Netzwerkzonen sind zusätzlich mit Firewalls geschützt.

Technische Sicherheitsmassnahmen

Innerhalb des geschützten Netzwerks von SPS läuft DIP über ein dediziertes Virtual Local Area Network (VLAN). Auf das VLAN kann nur via Multi-Faktor-Authentifizierung zugegriffen werden. Es besteht ein Log-Monitoring, um Logdateien in Echtzeit auszuwerten und alle Transaktionen nachzuvollziehen. Dank dem aktiven Netzwerk-Monitoring werden mögliche Cyberangriffe frühzeitig identifiziert und abgewehrt.

Physische Sicherheitsmassnahmen

Nur Mitarbeitende von SPS mit einem dafür vorgesehenen Badge haben Zutritt zu den Produktionsräumen von DIP. Die Mitarbeitenden unterstehen einer Geheimhaltungspflicht sowie dem Postgeheimnis. Die Zutritte werden protokolliert, und das Gebäude wird videoüberwacht. Bevor sie erweiterte Benutzerrechte erhalten, werden die Mitarbeitenden zusätzlich in einem Testverfahren (Screening) geprüft.

Internationale Sicherheitsstandards

Beim DIP gelten umfangreiche Sicherheitsrichtlinien, zum Beispiel die ISO-Norm 27001 für Informationssicherheit, in der Schweiz der Payment Card Industry Data Security Standard (PCI DSS) für Kreditkartentransaktionen sowie in den USA das Gesetz Health Insurance Portability and Accountability Act (HIPAA) für den Schutz von Gesundheitsinformationen. Die Einhaltung dieser Standards wird regelmässig überprüft.

Was ist Document Input Processing?
Mit Document Input Processing (DIP) optimiert Swiss Post Solutions dokumentenbasierte Geschäftsprozesse. Die Verarbeitungsprozesse sind hoch standardisiert und werden systematisch weiterentwickelt und verbessert. Von der Annahme und Aufbereitung von Dokumenten über das Scannen, die Indexierung und die Verarbeitung bis zur Archivierung bietet DIP alle Schritte, um unstrukturierte Daten automatisch aufzubereiten und sie ihren Kunden zur Verfügung zu stellen.
www.swisspostsolutions.com/dip

2020-072 (InfoSec) 05.2021

Post CH AG
Wankdorfallee 4
3030 Bern

Telefon 0848 888 888
E-Mail post@post.ch
www.post.ch

DIE POST

Document Output Processing
Sicheres Outputmanagement für Geschäftskunden

Mit dem Document Output Processing übernimmt Swiss Post Solutions für Geschäftskunden die Datenaufbereitung, den Druck und den Versand ihrer transaktionsbasierten Dokumente. Der Datenschutz ist dabei sichergestellt.

Hohe Verfügbarkeit

Document Output Processing (DOP) von Swiss Post Solutions (SPS) betreibt in grossen Briefzentren Produktionsstätten für die Datenaufbereitung, den Druck und den Versand von Dokumenten. Neben diversen Sicherungs- und Wiederherstellungsverfahren gibt es in den Produktionsstätten auch einen Notfallbetrieb, der bei einem ausserordentlichen Ereignis die Verfügbarkeit sicherstellt.

End-to-End-Verschlüsselung

Der Datenaustausch mit Kunden erfolgt beim DOP verschlüsselt und über ein Secure File Transfer Protocol (SFTP) und/oder über Virtual Private Network (VPN) Tunnel. Die Netzwerkzonen sind zusätzlich mit Firewalls geschützt.

Technische Sicherheitsmassnahmen

Innerhalb des geschützten SPS-Netzwerks läuft DOP über ein dediziertes Virtual Local Area Network (VLAN). Auf das VLAN kann nur via Multi-Faktor-Authentifizierung zugegriffen werden. Vollständiges Log-Monitoring wird eingesetzt, um Logdateien auszuwerten. Darüber hinaus werden alle Transaktionen nachvollziehbar und unanfechtbar abgespeichert. Externe zertifizierte Partner sorgen für einen normierten Vernichtungsprozess von Speichermedien.

Physische Sicherheitsmassnahmen

Nur Mitarbeitende von SPS mit einem dafür vorgesehenen Badge haben Zutritt zu den Produktionsräumen von DOP. Die Mitarbeitenden unterstehen einer Geheimhaltungspflicht sowie dem Postgeheimnis. Die Zutritte werden protokolliert, und das Gebäude wird videoüberwacht. Bevor sie erweiterte Benutzerrechte erhalten, werden Mitarbeitende ausserdem zusätzlich in einem Testverfahren (Screening) geprüft.

Internationale Sicherheitsstandards

Beim DOP gelten umfangreiche Sicherheitsrichtlinien, zum Beispiel die ISO-Norm 27001 für Informationssicherheit, in der Schweiz der Payment Card Industry Data Security Standard (PCI DSS) für Kreditkartentransaktionen sowie in den USA das Gesetz Health Insurance Portability and Accountability Act (HIPAA) für den Schutz von Gesundheitsinformationen. Die Einhaltung dieser Standards wird regelmässig überprüft.

Was ist Document Output Processing?
Mit Document Output Processing übernimmt Swiss Post Solutions für ihre Geschäftskunden den Druck und die Zustellung von transaktionsbasierten Geschäftsdokumenten wie Rechnungen, Policen oder Kontoauszügen. Die Dokumente können dem Endkunden physisch, digital oder in einem Mix aus beidem übermittelt werden. Die Automatisierung des Outputmanagements schont Ressourcen und garantiert gleichzeitig Stabilität, Sicherheit und Wirtschaftlichkeit. www.swisspostsolutions.com/dop

2020-072 (InfoSec) 05.2021

Post CH AG
Wankdorfallee 4
3030 Bern

Telefon 0848 888 888
E-Mail post@post.ch
www.post.ch

DIE POST

2020-072 (InfoSec) 05.2021

Post CH AG
Wankdorfallee 4
3030 Bern

Telefon 0848 888 888
E-Mail post@post.ch
www.post.ch

DIE POST