Sécurité de l'information à la Poste

En toute sérénité

Avant-propos

Marcel Zumbühl
CISO, la Poste

Chère cliente, cher client,

La sécurité de l'information est bien plus qu'une question de technique. Car la meilleure technique ne sert à rien en l'absence d'un élément: la confiance en elle. La Poste accorde une grande importance à vous procurer cette confiance et à vous conseiller et vous aider dans toutes vos questions relatives au thème de la sécurité de l'information.

Pour nous, la sécurité de vos données est primordiale. Cela commence dès le développement d'une offre, donc bien avant que vous puissiez utiliser nos produits et prestations en tant que client ou cliente. Et, bien sûr, nous veillons à ce que vos données soient sécurisées de manière appropriée et le restent pendant l'exploitation courante. Par exemple en soumettant nos produits à des tests réguliers et en surveillant l'exploitation jour et nuit dans nos centres de calcul.Ainsi, nous pouvons détecter à un stade précoce des tentatives d'attaques de hackers et prendre le cas échéant les mesures qui s'imposent.

Nous nous mettons en outre régulièrement à l'épreuve en collaboration avec des experts externes renommés. C'est ainsi que nous ainsi comment et où nous pouvons encore améliorer la sécurité pour notre clientèle. Le domaine de la sécurité ne marque jamais de pause. Le haut degré de qualité avec lequel la Poste gère la sécurité de l'information est confirmée par les certificateurs indépendants qui examinent et documentent chaque année nos mesures conformément à des normes de sécurité internationales.

Bien entendu, toutes les mesures de sécurité ont lieu en arrière-plan. Et elles poursuivent un unique objectif: pouvoir contribuer à votre succès avec un fonctionnement fiable et irréprochable de nos produits et de nos prestations, en vous donnant un sentiment de sécurité total.

Cordialement
Marcel Zumbühl, CISO, la Poste

Sécurité de l'information à la Poste

Le présent dossier contient différents factsheets relatifs à la sécurité de l'information de nos produits principaux et de nos prestations. Les informations publiées dans ce dossier sont contrôlées et modifiées en continu. Cela s'effectue en étroite collaboration entre la Gestion de produits, les responsables de la sécurité, la Communication et le Service juridique de la Poste. En cas de questions complémentaires, veuillez vous adresser à votre conseiller à la clientèle, à votre conseillère à la clientèle ou à Sécurité de l'information de la Poste.

Sécurité de l'information – menaces les plus fréquentes et contre-mesures

Les informations sont précieuses. C'est pourquoi elles doivent être protégées contre des auteurs d'attaques criminelles. Ces derniers tentent d'exploiter les vulnérabilités pour s'octroyer des avantages indus. Dans ce cadre, les attaques courantes sont le vol d'informations, le hameçonnage (phishing) et l'abus d'identités, la destruction et la manipulation d'informations ainsi que les attaques de surcharge contre des centres de calcul.

Vol d'informations

Procédure: Les criminels s'immiscent dans les systèmes informatiques, dérobent des informations et les vendent sur le marché noir. Les cibles favorites sont les informations personnelles, les données d'entreprise, les données de cartes de crédit et, de manière générale, les informations liées à des processus financiers. Souvent, les criminels essaient de gagner la confiance de la victime en indiquant des fausses identités pour accéder ainsi au bon endroit.

Évaluation: Ce modèle d'attaque est moyennement répandu. Il requiert des connaissances techniques élevées ou les outils professionnels correspondants. En outre, l'agresseur doit disposer de l'accès à un réseau de receleurs pour pouvoir vendre les données.

Contre-mesures: Les systèmes dans les centres de calcul de la Poste sont protégés par plusieurs niveaux de protection et placés sous une surveillance permanente. Des points faibles sont recherchés en continu aux fins d'élimination ou de restriction avec des mesures supplémentaires.

Phishing et vol d'identité

Procédure: Les criminels gagnent la confiance de la victime par le biais de faux e-mails, de messages texte, voire d'appels téléphoniques, et usurpent l'identité numérique de la personne. Ils peuvent également acheter les identités de victimes (p. ex. accès aux comptes) sur le marché noir. À l'aide de l'identité dérobée, ils essaient de commander des marchandises, de manipuler des prestations ou de dévaliser directement des comptes bancaires.

Évaluation: Répandu dans le monde entier et ne requiert pas de grandes compétences techniques de l'agresseur. Généralement, ce type d'attaque a lieu par vagues.

Contre-mesures: Le succès de la lutte contre les vols d'identité et le phishing requiert une grande vigilance et une réaction rapide, aussi bien de la part de la clientèle que de la part de la Poste. Les attaques peuvent être détectées et bloquées sur la base d'écarts minimes dans le texte et la langue ou dans le comportement de systèmes.

Manipulation des données et perte d'informations

Procédure: Les criminels pénètrent dans des systèmes, créent une copie des informations et détruisent l'original ou le chiffrent de sorte qu'il ne soit plus accessible. En-suite, ils font chanter la victime en utilisant l'information dérobée ou le moyen d'accès aux données comme moyen de pression.

Évaluation: Les attaques sont généralement réalisées de manière ciblée. Elles nécessitent des connaissances techniques approfondies ainsi que des connaissances détaillées sur la victime.

Contre-mesures: Pour se défendre contre de telles attaques, la Poste utilise toute une série de mécanismes de protection. Elle collabore également de manière étroite avec les autorités de poursuite pénale. Ainsi, elle peut réagir avec détermination dès la tentative d'attaque.

Attaques de surcharge contre les infrastructures

Procédure: Des criminels s'attaquent de manière ciblée à l'accès à une prestation jusqu'à ce que celle-ci soit surchargée et ne puisse plus être utilisée via Internet. Ensuite, ils font chanter la victime et exigent de l'argent pour éliminer la situation de surcharge.

Évaluation: Les attaques ont lieu de manière sporadique, généralement sous forme de tentatives pour tester la résistance des mécanismes de protection. Les attaques requièrent des connaissances techniques approfondies et une infrastructure dédiée performante.

Contre-mesures: En collaboration avec des prestataires de réseau, la Poste dispose de mécanismes de protection régulièrement contrôlés afin de pouvoir se défendre contre les attaques de surcharge.

Voici comment renforcer votre protection

Les règles principales pour davantage de sécurité:
- Utilisez des mots de passe sûrs
- Effectuez régulièrement des mises à jour
- Protégez votre connexion réseau et votre connexion Internet
- Chiffrez vos données
- En cas d'e-mails et de demandes suspects, faites preuve de prudence

Vous trouverez également des informations actuelles relatives à la sécurité de l'information sur les sites web officiels d'organisations spécialisées. Nous pouvons vous recommander les sites suivants:

- Centre national pour la cybersécurité NSCS (auparavant MELANI) – www.ncsc.admin.ch
- Swiss Cyber Experts – www.swiss-cyber-experts.ch
- ICT Switzerland – www.ictswitzerland.ch
- ebas.ch – www.ebas.ch

Protection des données

Dans le cadre de la fourniture de prestations à ses clients, la Poste attache une grande importance à un traitement des données personnelles responsable et conforme à la loi.

La Poste garantit que les données sont traitées avec le plus grand soin, conformément aux dispositions légales en vigueur relatives à la protection des données et à la législation postale.

La Poste dispose d'un système complet de gestion de la protection des données et examine chaque prestation à l'aune de sa conformité en matière de protection des données.

Sécurité certifiée

La Poste se fait certifier dans des thèmes clés sur des normes reconnues internationalement. Ainsi, elle respecte les bonnes pratiques et simplifie les processus de compliance des clients. Il s'agit notamment des normes suivantes:

ISO 27001
La norme internationale spécifie les exigences relatives à la configuration, à la mise en place, à la maintenance et à l'amélioration continue d'un système de gestion de la sécurité de l'information (ISMS).

ISO 22301
La norme internationale spécifie les exigences relatives à la création et la gestion d'un Business Continuity Management System (BCMS) efficace.

TÜV Trusted Site Infrastructure TSI V3.2 Dual Site Level 3
Les deux centres de calcul de la Poste sont localisés en Suisse dans des sites géographiquement indépendants. Ils offrent un environnement d'hébergement d'excellente qualité doté de plusieurs niveaux de sécurité. Le certificat définit les exigences posées à l'infrastructure physique d'un centre de calcul (site, construction du bâtiment, technique de sécurité, alimentation en énergie et technique de réfrigération) et aux processus organisationnels de l'exploitant. En outre, il documente l'aptitude relative aux domaines de sécurité pour lesquels une grande disponibilité est exigée.

ISAE 3402
PostFinance en sa qualité d'établissement financier et Swiss Post Solutions en tant que fournisseur de services pour les établissements financiers ainsi que Informatique Poste sont soumis à un contrôle et à une certification conformément à l'International Standard on Assurance Engagements (ISAE) 3402 en matière d'efficacité de contrôle du système de contrôle interne.

PCI DSS
Le Payment Card Industry Data Security Standard (PCI DSS) a été conçu par le PCI Security Standards Council afin d'enrayer les escroqueries concernant les paiements par carte de crédit sur Internet.

Postshop
Faire ses achats en toute sécurité dans la boutique en ligne de la Poste

Sur postshop.ch, de nombreuses offres qui facilitent le quotidien peuvent être commandées en un clic. La sécurité lors des achats est garantie par le chiffrage des informations et une plateforme de paiement certifiée.

Différentes possibilités d'accès

Les personnes souhaitant faire des achats sur Postshop peuvent se connecter via le Login client Poste ou avec SwissID, mais également commander en tant que visiteur. Toutefois, le paiement sur facture et l'utilisation de bons sont réservés aux clients enregistrés. En outre, les cartes cadeaux et les bons électroniques ne peuvent pas être achetés sur facture. Ces mesures renforcent la protection contre d'éventuelles tentatives d'escroquerie.

Disponibilité élevée

Au premier semestre 2020, le Postshop était disponible à 99,5%. Afin de pouvoir également réagir à des volumes importants, la Poste réalise périodiquement des tests de charge. En outre, elle évalue la disponibilité par le biais d'un monitoring actif et contrôle si les indices de référence définis sont respectés.

Système de paiement sécurisé

Les données des clients du Postshop sontexclusivement stockées en Suisse. Les personnes payant par carte de crédit sont transférées de Postshop vers BillingOnline, la plateforme de paiement sécurisée et certifiée PCI DSS. Cette norme de sécurité internationale protège les données concernées contre le cybervol et l'utilisation frauduleuse. Chaque trafic réseau via Internet a lieu de manière cryptée.

Tests complets

La Poste contrôle et optimise son Postshop en continu. D'une part, Postshop est représenté dans le programme bug bounty de la Poste. Cela signifie que d'éventuels points faibles identifiés (findings) peuvent être corrigés immédiatement. D'autre part, la Poste soumet régulièrement ses ordinateurs et ses réseaux à un test de sécurité complet, en conformité avec des normes internationales (OWASP Top 10). En outre, la Poste analyse périodiquement le besoin en protection et le concept de sécurité de l'information et de protection des données et fait effectuer des tests de sécurité par un service de contrôle indépendant avant chaque grande mise à jour du Postshop.

Qu'est-ce que Postshop?
Postshop est la boutique en ligne de la Poste. Il propose des marchandises et des services qui ont un lien avec l'activité de la Poste: des smartphones aux accessoires de voyage en passant par les cartes cadeaux. Même les timbres-poste les plus récents de la Poste, ainsi que le matériel d'emballage et de mise sous pli pour les lettres et les colis peuvent être commandés facilement en quelques clics. www.postshop.ch

2020-072 (InfoSec) 05.2021

Poste CH SA
Wankdorfallee 4
3030 Berne

Téléphone 0848 888 888
E-mail post@poste.ch
www.poste.ch

LA POSTE

Prestations de distribution
Pratiques et sûres

La Poste et ses prestations de distribution proposent à la clientèle commerciale et à la clientèle privée de nombreuses possibilités pour gérer aisément la réception de courrier.

Identification personnelle

Les prestations de distribution de la Poste sont à la disposition de l'ensemble de la clientèle de la Poste. Une identification personnelle est obligatoire pour leur utilisation. Les clients commerciaux doivent en outre présenter un justificatif, par exemple un extrait du RC ou des statuts d'association. La Poste confirme uniquement qu'elle a bien vu les documents d'identification. Elle ne conserve, ni archive les documents.

Flux de données entièrement automatisé

Les données relevées dans le cadre de ces prestations sont transmises de manière entièrement automatisée via une application centralisée à la Poste. Cette procédure garantit que tous les services concernés disposent toujours des données actuelles. Les données restent au sein de la Poste.

Accès strictement réglementé

Seuls les collaborateurs de la Poste disposant des droits d'utilisateur spécifiques ont accès aux prestations de distribution ou à l'application centralisée qui sauvegarde les données nécessaires pour les services. Si un utilisateur est inactif pendant 90 jours, son autorisation est automatiquement supprimée.

Se protéger soi-même

Les clients peuvent renforcer leur protection en choisissant un mot de passe le plus complexe possible pour le Login client Poste et en ne le sauvegardant pas dans le navigateur, ni en le communiquant à des tiers.

En quoi consistent les prestations de distribution?
Ouvrir et administrer des demandes de réexpédition, modifier des adresses ou communiquer des déménagements: ce ne sont que quelques-unes des nombreuses prestations de distribution que la Poste propose à sa clientèle. Elles peuvent être utilisées 24 heures sur 24 en ligne (ordinateur, smartphone, tablette) via le Login client Poste ou pendant les horaires d'ouverture au guichet, ou encore via le service à la clientèle.
www.poste.ch/reception

2020-072 (InfoSec) 05.2021

Poste CH SA
Wankdorfallee 4
3030 Berne

Téléphone 0848 888 888
E-mail post@poste.ch
www.poste.ch

LA POSTE

PubliBike
Se déplacer en toute sécurité

PubliBike permet d'emprunter des vélos et des vélos électriques dans toute la Suisse. L'inscription requiert un login, la facturation s'effectue à la minute, le paiement a lieu par carte de crédit. La Poste veille à ce que ce service soit et reste sûr.

La redondance garantit la disponibilité

Les données de PubliBike sont enregistrées dans deux centres de calcul certifiés ISO 27001. Si un centre de calcul tombe en panne, la redondance garantit que les données et l'exploitation de PubliBike sont assurées.

Les interactions avec la clientèle ont lieu via différents serveurs, ce qui permet d'éviter une trop grande charge d'un serveur donné.

Gestion confidentielle des données

La Poste accorde une grande importance à la protection des données personnelles. Elle les traite donc avec le plus grand soin, conformément aux dispositions légales en vigueur relatives à la protection des données et à d'autres bases légales. L'ensemble du trafic des données via Internet a lieu de manière cryptée.

Mesures de sécurité

À l'aide d'un système d'identification des attaques, des modifications non autorisées effectuées sur les systèmes de PubliBike sont immédiatement détectées, examinées et bloquées. En outre, les systèmes sont contrôlés régulièrement à la recherche de points faibles, notamment avec un test de sécurité complet, en conformité avec des normes internationales (OWASP Top 10). L'utilisation des composants de système est enregistrée dans un journal pour le suivi et contrôlée en termes d'irrégularités.

Qu'est-ce que PubliBike?
Publibike est le plus grand service de bike-sharing de Suisse. Elle complète idéalement les transports publics et privés pour les courtes distances et permet de diminuer l'engorgement des centres urbains tout en favorisant la santé des usagers. PubliBike se prête également à la mise en réseau d'infrastructures comme les universités, les administrations ou encore les grands sites industriels. www.publibike.ch

2020-072 (InfoSec) 05.2021

Poste CH SA
Wankdorfallee 4
3030 Berne

Téléphone 0848 888 888
E-mail post@poste.ch
www.poste.ch

LA POSTE

Document Input Processing
Scanner et préparer des documents en toute sécurité

Avec Document Input Processing (DIP), Swiss Post Solutions traite pour ses clients commerciaux des données non structurées issues de documents entrants physiques et électroniques, la protection des données étant assurée à tout moment.

Disponibilité élevée

Par le biais de différentes mesures, Swiss Post Solutions (SPS) assure une disponibilité maximale des services. Cela comprend notamment une infrastructure de centre de calcul réfléchie, des tests de restauration réguliers et des sauvegardes de bases de données ainsi qu'une connexion au réseau redondante des sites avec des mécanismes «fail over». Ces derniers garantissent qu'en cas de panne d'ordinateur, le deuxième ordinateur prend en charge les tâches du premier sans interruption.

Chiffrement de bout en bout

L'échange de données avec la clientèle s'effectue, avec Document Input Processing (DIP), toujours de manière chiffrée via un Secure File Transfer Protocol (SFTP) et/ou un Virtual Private Network (VPN) Tunnel. En outre, les zones de réseau sont protégées par des pare-feu (firewalls).

Mesures de sécurité techniques

Au sein du réseau protégé de SPS, DIP s'exécute sur un Virtual Local Area Network (VLAN) dédié. L'accès au VLAN s'effectue uniquement via une authentification multifactorielle. Il existe un monitoring journal pour évaluer les fichiers journal en temps réel et retracer toutes les transactions. Le monitoring de réseau actif permet d'identifier à un stade précoce d'éventuelles cyberattaques et de les repousser.

Mesures de sécurité physiques

Seuls les collaborateurs de SPS munis d'un badge prévu à cet effet ont accès aux locaux de production de DIP. Tous les collaborateurs sont soumis à une obligation de confidentialité ainsi qu'au secret postal. Les accès sont consignés et le bâtiment est surveillé par vidéo. Avant d'obtenir des droits d'utilisateur élargis, les collaborateurs sont en outre soumis à un contrôle dans une procédure de test (screening).

Normes de sécurité internationales

Des directives de sécurité exhaustives s'appliquent pour DIP, par exemple la norme ISO 27001 pour la sécurité de l'information, le Payment Card Industry Data Security Standard (PCI DSS) pour les transactions par cartes de crédit en Suisse ainsi que la loi américaine Health Insurance Portability and Accountability Act (HIPAA) pour la protection des informations sur la santé. Le respect de ces normes est vérifié dans le cadre d'audits réguliers.

Qu'est-ce que Document Input Processing?
Avec Document Input Processing (DIP), Swiss Post Solutions optimise les processus d'affaires basés sur les documents. Les processus de traitement sont ultra-standardisés et systématiquement développés et améliorés. Du dépôt et de la préparation de documents à l'archivage en passant par le scannage, l'indexation et le traitement, DIP offre toutes les étapes pour préparer automatiquement des données non structurées et les mettre à la disposition de ses clients.
www.swisspostsolutions.com/dip

2020-072 (InfoSec) 05.2021

Poste CH SA
Wankdorfallee 4
3030 Berne

Téléphone 0848 888 888
E-mail post@poste.ch
www.poste.ch

LA POSTE

Document Output Processing
Gestion de l'output sécurisée pour les clients commerciaux

Avec Document Output Processing, Swiss Post Solutions prend en charge pour les clients commerciaux la préparation des données, l'impression et l'expédition de leurs documents basés sur les transactions, la protection des données étant assurée à tout moment.

Disponibilité élevée

Document Output Processing (DOP) de Swiss Post Solutions (SPS) exploite dans de grands centres courrier des sites de production pour la préparation des données, l'impression et l'expédition de documents. En plus de différents procédés de sauvegarde et de restauration, les sites de production disposent également d'une exploitation d'urgence qui assure la disponibilité en cas d'événement exceptionnel.

Chiffrement de bout en bout

Avec DOP, l'échange de données avec la clientèle s'effectue toujours de manière chiffrée et via un Secure File Transfer Protocol (SFTP) et/ou via un Virtual Private Network (VPN) Tunnel. En outre, les zones de réseau sont protégées par des pare-feu (firewalls).

Mesures de sécurité techniques

Au sein du réseau protégé de SPS, DOP s'exécute sur un Virtual Local Area Network (VLAN) dédié. L'accès au VLAN s'effectue uniquement via une authentification multifactorielle. Un monitoring journal complet est utilisé pour évaluer les fichiers journal. En outre, toutes les transactions sont sauvegardées de manière retraçable et juridiquement inattaquable. Des partenaires externes certifiés assurent un processus d'élimination normé des supports de données.

Mesures de sécurité physiques

Seuls les collaborateurs de SPS munis d'un badge prévu à cet effet ont accès aux locaux de production de DOP. Tous les collaborateurs sont soumis à une obligation de confidentialité ainsi qu'au secret postal. Les accès sont consignés et le bâtiment est surveillé par vidéo. En outre, avant d'obtenir des droits d'utilisateur élargis, les collaborateurs sont soumis à un contrôle dans une procédure de test (screening).

Normes de sécurité internationales

Des directives de sécurité exhaustives s'appliquent pour DIP, par exemple la norme ISO 27001 pour la sécurité de l'information, le Payment Card Industry Data Security Standard (PCI DSS) pour les transactions par cartes de crédit en Suisse ainsi que la loi américaine Health Insurance Portability and Accountability Act (HIPAA) pour la protection des informations sur la santé. Le respect des normes est vérifié dans le cadre d'audits réguliers.

Qu'est-ce que Document Output Processing?
Avec Document Output Processing, Swiss Post Solutions prend en charge pour ses clients commerciaux l'impression et la distribution de documents commerciaux basés sur les transactions tels que les factures, les polices ou les extraits de compte. Les documents peuvent être transmis au client final par voie physique, numérique ou dans un mélange de ces deux possibilités. L'automatisation de la gestion de l'output préserve les ressources tout en garantissant la stabilité, la sécurité et la rentabilité.
www.swisspostsolutions.com/dop

2020-072 (InfoSec) 05.2021

Poste CH SA
Wankdorfallee 4
3030 Berne

Téléphone 0848 888 888
E-mail post@poste.ch
www.poste.ch

LA POSTE

2020-072 (InfoSec) 05.2021

Poste CH SA
Wankdorfallee 4
3030 Berne

Téléphone 0848 888 888
E-mail post@poste.ch
www.poste.ch

LA POSTE