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 cliente ou client. Et bien sûr, pendant l'exploitation courante, nous veillons à ce que vos données soient sécurisées et le restent. 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 identifions 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 confirmé par les principaux organismes de certification indépendants, qui examinent et évaluent 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: nous permettre de 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.

Sincères salutations
Marcel Zumbühl, CISO, la Poste

Sécurité de l’information à la Poste

Cette brochure contient différents factsheets relatifs à la sécurité de l’information concernant nos produits principaux et nos prestations. Les informations publiées ici 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. Pour toute autre question, veuillez vous adresser à votre conseillère ou à votre conseiller à la clientèle.

Sécurité de l’information – menaces les plus fréquentes et mesures correctives

Les informations sont précieuses. C’est pourquoi nous devons les protéger des attaques criminelles. Les agresseurs (hackers) 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’usurpation d’identité, la destruction et la manipulation d’informations ainsi que les attaques de surcharge contre des centres de calcul.

Vol d’informations

Méthode: 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 de fausses identités pour accéder ainsi à l’endroit souhaité.

Analyse: Ce procédé est de plus en plus répandu. Il requiert des connaissances techniques en la matière ou les outils professionnels correspondants. En outre, l’agresseur doit disposer de l’accès à un réseau de receleurs pour pouvoir vendre les données.

Mesures correctives: Les systèmes dans les centres de calcul de la Poste ainsi que les environnements cloud utilisés par la Poste sont protégés à plusieurs niveaux et placés sous une surveillance permanente. La Poste recherche en continu des points faibles afin de les éliminer ou de les limiter avec des mesures supplémentaires.

Phishing et vol d’identité

Méthode: Les criminels gagnent la confiance de la victime par le biais de faux e-mails, de messages texte ou 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.

Analyse: Ces pratiques sont largement répandues dans le monde entier et ne requièrent pas de grandes compétences techniques pour l’agresseur. Généralement, ce type d’attaque a lieu par vagues.

Mesures correctives: 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. Une incitation à une action inhabituelle ou une incohérence au niveau d’une transaction peut laisser penser à une attaque. Il est dès lors possible de la contrer.

Manipulation des données et perte d’informations

Méthode: 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. Ensuite, ils font chanter la victime en utilisant l’information dérobée ou le moyen d’accès aux données comme élément de pression.

Analyse: Généralement réalisées de manière ciblée, ces attaques nécessitent des connaissances approfondies sur le plan technique et au sujet de la victime.

Mesures correctives: 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

Méthode: Des criminels s'attaquent de manière ciblée à des services en ligne jusqu'à ce que ceux-ci soient surchargés et ne puissent plus être utilisés via Internet; c'est ce que l'on appelle des «Denial of Service Attacks», ou «DOS». Puis, ils font chanter la victime et exigent de l'argent pour éliminer la surcharge.

Analyse: Ces attaques ont lieu de manière sporadique, généralement sous forme de tentatives pour tester la résistance des mécanismes de protection. Elles requièrent des connaissances techniques approfondies et une infrastructure solide du côté du hacker.

Mesures correctives: 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:
– Sauvegardez vos données sur des supports indépendants
– Utilisez des mots de passe complexes et, si possible, une authentification à deux facteurs
– Assurez-vous que votre logiciel est à jour (dernière mise à jour installée)
– Protégez votre connexion réseau et votre connexion Internet
– En cas d'e-mails et de demandes suspects, faites preuve de prudence
– Sensibilisez vos collaboratrices et vos collaborateurs

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 NCSC (auparavant MELANI) – www.ncsc.admin.ch
– Swiss Cyber Experts – www.swiss-cyber-experts.ch
– Digitalswitzerland – www.digitalswitzerland.com
– E-banking en toute sécurité – 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

Depuis plusieurs années, la Poste passe des certifications dans des domaines clés pour obtenir des normes reconnues à l'échelle internationale. Ainsi, elle respecte les bonnes pratiques et simplifie les processus de compliance des clients. Il s'agit notamment des normes suivantes:

ISO 27001
Norme internationale relative 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 (SGSI)

ISO 22301
Norme internationale concernant la création et la gestion d'un système effectif de Business Continuity Management (BCMS)

ISO 20000-1
Norme internationale relative à la gestion de services en informatique

TÜV Trusted Site Infrastructure TSI V3.2 Dual Site Level 3
Les deux centres de calcul de la Poste sont localisés en Suisse sur des sites géographiquement indépendants. Ils of-frent un environnement d'hébergement d'excellente qualité doté de plusieurs niveaux de sécurité. Le certificat porte sur l'infrastructure physique d'un centre de calcul (site, construction du bâtiment, technique de sécurité, alimentation en énergie et technique de réfrigération) et les processus organisationnels de l'exploitant.

ISAE 3402
PostFinance et l'unité Informatique de la Poste sont soumises 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 en lien avec les paiements par carte de crédit sur Internet.

Mes envois

Gestion pratique des envois postaux selon les besoins individuels des clients

Description du produit

Avec «Mes envois», la clientèle privée de la Poste peut gérer la réception de ses envois. La Poste l'informe automatiquement et à l'avance de l'arrivée de colis et de lettres recommandées. Tous les envois peuvent être consultés dans le Centre clientèle dans l'application ou sur la page d'accueil de la Poste, sous «Mes envois». Qu'il s'agisse d'un envoi ponctuel ou d'un ordre permanent, la clientèle peut configurer ses envois à sa guise avant la distribution. Elle peut par exemple régler les taxes douanières en amont, réexpédier l'envoi ou encore déterminer un deuxième lieu et une deuxième date de distribution. Il lui est également possible de sélectionner des options pour les envois manqués. «Mes envois» offre plus de flexibilité et une meilleure transparence en matière de réception des envois.

Disponibilité

Le service «Mes envois» est disponible 24h/24, 7j/7. Les clientes et les clients peuvent gérer les modalités de réception de leurs envois partout et à tout moment. En outre, le système de surveillance permanente de l'application permet d'identifier rapidement d'éventuels dysfonctionnements et de les éliminer.

Confidentialité

La Poste protège les données personnelles, les données d'envoi et le contenu des factures contre tout accès non autorisé. Il en va de même avec «Mes envois»: ainsi, seuls les membres du personnel de la Poste qui ont besoin de ces informations pour l'accomplissement de leurs tâches y ont accès.

Intégrité

La clientèle peut compter sur le fait que ses données sont modifiées uniquement dans le cadre de sa commande. Pour permettre à la clientèle de modifier ses paramètres de distribution, la Poste met à sa disposition une procédure sécurisée de connexion au site web ou à l'application.

Traçabilité

Un envoi effectue un long chemin pour parvenir à sa ou son destinataire. Toutes les modifications apportées entre-temps aux modalités de distribution de l'envoi sont enregistrées. Ce faisant, la Poste s'assure que seules les personnes autorisées puissent procéder à des modifications.

2020-072 (InfoSec) 06.2023

Accès/Identification

Les clientes et les clients peuvent consulter le statut d'un envoi à l'aide du numéro d'envoi sans devoir se connecter à la Post-App ou au site poste.ch. S'ils souhaitent obtenir plus de détails sur l'envoi ou modifier un paramètre, ils doivent se connecter avec leur nom et leur mot de passe. Ce login peut être créé de manière simple et sécurisée grâce à SwissID. Dans des cas particuliers (par exemple en cas de changement d'adresse), un code de confirmation est envoyé à l'adresse e-mail enregistrée par la personne. Ce code sert d'élément de sécurité supplémentaire; on parle alors d'authentification à deux facteurs, qui permet à la Poste d'écarter toute tentative d'escroquerie en cas de demande de modification.

Comment la clientèle peut-elle se protéger?

Les données personnelles et les informations qui y sont associées doivent faire l'objet d'une protection particulière. Le simple fait de se connecter aux services sécurisés de la Poste (par exemple via poste.ch ou la Post-App) constitue déjà une protection de base solide. La clientèle peut renforcer le niveau de sécurité en paramétrant des mots de passe personnels complexes, et en ne les partageant avec personne pour une protection maximale. Si des clientes et des clients relèvent une incohérence avec leurs données, la Poste réagit rapidement en les aidant de manière simple sur poste.ch, dans l'application ou dans la filiale la plus proche.

2020-072 (InfoSec) 06.2023

Post-App

Les principales informations et prestations de la Poste en un clic. Partout et à tout moment.

Description du produit

Grâce à la Post-App de la Poste, la clientèle a accès 24 heures sur 24 aux principales prestations et informations de la Poste. Les clientes et les clients accèdent à la Post-App via un login personnel. Cette application propose notamment les services suivants: Mes envois (p. ex. suivi des envois, invitation à retirer un envoi, pick@home, Garder le courrier), recherche de site, Codescanner et vidéo Webstamp. Les services sont régulièrement enrichis et adaptés aux besoins de la clientèle.

Disponibilité

La Post-App est disponible sur les App Stores de Google et d'Apple et fonctionne sur les appareils Android et iOS. Au niveau de la clientèle, la disponibilité de la Post-App dépend de l'accès mobile ou fixe à Internet et, le cas échéant, de la performance de l'appareil mobile utilisé. En général, la Post-App et les services qu'elle propose sont facilement accessibles.

Confidentialité

La Post-App, disponible via les App Stores officiels, présente un haut niveau de confidentialité, car il s'agit d'un développement propre à la Poste. Les connexions et l'échange de données entre l'application et les services connectés sont cryptés. Les données sensibles telles que les adresses clients, les données d'envoi, etc. ne sont pas enregistrées localement dans l'application. Pour pouvoir utiliser des fonctionnalités protégées dans la Post-App, les utilisatrices et les utilisateurs doivent se connecter avec un nom d'utilisateur et un mot de passe, ce qui renforce encore la sécurité.

Intégrité

Le chiffrement des connexions et de l'échange de données entre l'application et les services connectés garantit l'intégrité des données. En outre, l'application vérifie l'origine des données à l'aide d'un mécanisme de sécurité supplémentaire (certificat).

Traçabilité

Les activités effectuées dans les services connectés de la Poste sont consignées avec une traçabilité parfaite.

Accès/Identification

Pour pouvoir utiliser les fonctionnalités protégées dans la Post-App, il faut disposer d'un compte utilisateur Poste avec un nom d'utilisateur et un mot de passe. Les données de connexion sont transmises sous forme cryptée. Les fonctionnalités étendues de la Post-App sont protégées par un login SwissID.

2020-072 (InfoSec) 06.2023

Comment la clientèle peut-elle se protéger?

Il est conseillé à la clientèle de sécuriser l'appareil mobile utilisé au moyen d'un NIP, d'une reconnaissance faciale ou d'une empreinte digitale, pour éviter qu'en cas de perte ou de vol de l'appareil et en l'absence de protection, des tiers n'accèdent aux informations clients (notamment sur la Post-App).

Il est recommandé de télécharger la Post-App exclusivement via les App Stores officiels d'Android ou d'Apple.

Il est déconseillé de supprimer sans autorisation préablable les restrictions d'utilisation de l'appareil utilisé (ce que l'on appelle le jailbreaking). Les restrictions d'utilisation sont volontairement mises en place par les fabricants pour des raisons de sécurité. En cas de suppression de ces dernières, l'appareil peut faire l'objet d'un accès non autorisé, ce qui peut entraîner par exemple le vol de données ou l'accès à des applications bancaires.

2020-072 (InfoSec) 06.2023

Postshop

Shopping sécurisé sur le Postshop.
Des offres variées en un clic.

Description du produit

Le Postshop (postshop.ch) est la boutique en ligne de la Poste. Il propose des produits en lien avec les activités postales qui simplifient le quotidien de la clientèle: des smartphones aux articles de bureau et à la papeterie, en passant par les cartes cadeaux. Il est même possible de commander facilement en ligne les derniers timbres de la Poste, ainsi que le matériel d'emballage et de mise sous pli des lettres et des colis. Les achats sont sécurisés par le biais du chiffrement des informations et d'une plateforme de paiement certifiée.

Disponibilité

Le Postshop fonctionne 24h/24, avec de très rares périodes d'indisponibilité. La Poste réalise périodiquement des tests de charge et vérifie si les valeurs cibles sont respectées à l'aide d'un monitoring actif.

Confidentialité

La Poste s'assure que les données ne puissent être consultées ou publiées que par les personnes qui en ont l'autorisation. Elle analyse périodiquement le besoin de protection ainsi que son concept d'autorisation d'accès pour la boutique en ligne. La Poste applique une gestion prudente des données et met en œuvre les directives de la déclaration de protection des données ainsi que les prescriptions légales.

Intégrité

La Poste contrôle et optimise sa boutique en ligne en continu. Avant chaque mise à jour majeure, elle charge un service indépendant de réaliser des tests de sécurité conformes aux normes internationales (OWASP Top 10). En outre, le Postshop fait partie du programme bug bounty de la Poste, dans le cadre duquel des hackers éthiques sont chargés par la Poste d'identifier les failles de sécurité, qu'elle corrige alors immédiatement.

Traçabilité

Un système de surveillance (monitoring) permet d'écarter tout risque de modification des données client par des tiers dans le Postshop.

Accès/Identification

Les personnes souhaitant faire des achats sur le Postshop peuvent se connecter avec SwissID ou passer commande en tant que visiteur. Toutefois, les achats sur facture et l'utilisation de bons sont réservés à la clientèle enregistrée. Dans tous les cas, certaines marchandises comme les cartes cadeaux ou les bons électroniques doivent faire l'objet d'un paiement immédiat. Ces mesures renforcent la protection contre d'éventuelles tentatives d'escroquerie.

2020-072 (InfoSec) 06.2023

Comment la clientèle peut-elle se protéger?

La sécurité de base est assurée par le traitement méticuleux du mot de passe SwissID ainsi que des données de la carte PostFinance, de la carte bancaire ou de la carte de crédit. Le mot de passe doit être difficile à deviner et doit être exclusivement utilisé pour SwissID. Afin de renforcer le niveau de sécurité, l'idéal est que la clientèle se connecte directement sur le portail de la Poste. Cette procédure est plus sûre qu'un clic sur un lien dans un e-mail (non attendu), qui pourrait être une tentative de hameçonnage.

2020-072 (InfoSec) 06.2023

Dédouanement de marchandises et d'envois

Des procédures sécurisées lors de l'importation et de l'exportation de marchandises et d'envois garantissent un traitement efficace, une livraison rapide ainsi qu'une gestion sûre des données sensibles.

Description du produit

Pratiquement tous les opérateurs postaux – dont la Poste – sont affiliés à l'Union postale universelle (UPU) et respectent ses prescriptions, y compris en matière de conditions de livraison et de thèmes de facturation. Aux services postaux habituels s'ajoutent des prestations douanières et fiscales. À cet égard, la Poste doit établir ou obtenir les documents pertinents afin de pouvoir effectuer une déclaration pour le dédouanement. Sur la base des informations relatives à l'envoi, la valeur et donc le montant des droits de douane sont déterminés. Ce processus évolue lui aussi et se numérise de plus en plus.

Disponibilité

La clientèle a la possibilité de saisir les informations nécessaires à la déclaration de l'envoi (p. ex. contenu, poids et valeur) au guichet ou par voie numérique (p. ex. via le compte utilisateur sous poste.ch ou via la Post-App). Les possibilités numériques permettent aux clientes et aux clients de ne plus dépendre de lieux ou d'heures d'ouverture et de procéder aux inscriptions en toute flexibilité – au moment qui leur convient le mieux et même depuis chez eux.

Confidentialité

La Poste protège les données personnelles, les données d'envoi et le contenu des factures contre tout accès non autorisé. Elle traite les données clients et les met également à la disposition des autorités douanières, ce qui est son obligation. Lors du suivi des envois ou de la facturation, l'échange sécurisé de données entre la clientèle et la Poste est indispensable. C'est ce que garantissent les logins clients, les sites web contrôlés et les connexions cryptées avec les partenaires externes.

Intégrité

Notre clientèle peut exiger que ses données ne soient modifiées que par la Poste et uniquement dans des cas justifiés. C'est le cas, par exemple, lorsque des adaptations doivent être apportées au nom, à l'adresse ou aux données du compte. Pendant tout le traitement, les données sont protégées et sécurisées.

Traçabilité

Le trajet d'un envoi jusqu'à la personne qui le reçoit est long – surtout à l'importation et à l'exportation. L'envoi est scanné à chaque étape du traitement. Lors du dédouanement, la traçabilité ainsi garantie est un facteur essentiel pour que l'envoi soit transporté dans de bonnes conditions et que les droits de douane soient calculés correctement.

2020-072 (InfoSec) 06.2023

Accès/Identification

La Poste ne cesse de développer ses points de contact physiques et numériques. À cet égard, elle doit garantir l'identité de sa clientèle. C'est le seul moyen pour la Poste de communiquer avec ses clientes et clients sur des contenus importants (comme l'envoi) ou de leur faire parvenir des informations sensibles qui leur sont uniquement destinées. Cela peut se faire par un login client sur poste.ch ou par la présentation de la pièce d'identité dans la filiale. L'identification est la clé de l'accès à nos services et aux données associées.

Comment la clientèle peut-elle se protéger?

Les fraudeuses et les fraudeurs tentent d'obtenir les informations de cartes de crédit de tiers par hameçonnage. Souvent, ils y parviennent en demandant à ces derniers de payer une facture en souffrance. Cette méthode pourrait également être utilisée pour les données d'envoi. La Poste invite donc à la plus grande prudence. Si les clientes et clients concernés n'ont pas déposé d'envoi à la Poste ou n'attendent pas de commande, il leur est conseillé d'ignorer ces e-mails de phishing. Si un envoi a effectivement été déposé ou est attendu, le mieux est de consulter la facture sur le compte utilisateur de la Poste. Notre clientèle peut également s'adresser à la filiale de la Poste la plus proche. De cette manière, elle aura l'assurance que la facture provient effectivement de la Poste et qu'elle est donc en bonne et due forme.

Si quelque chose semble inhabituel dans les envois de lettres et de colis, il est également possible de se faire conseiller auprès des filiales ou du Contact Center. Si certains de nos clientes et clients pensent avoir probablement cliqué trop vite sur un e-mail, il leur est conseillé de changer immédiatement de mot de passe ou d'utiliser l'authentification à deux facteurs.

2020-072 (InfoSec) 06.2023

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.

Description du produit

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.

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.

2020-072 (InfoSec) 06.2023

2020-072 (InfoSec) 04.2023

Poste CH SA
Wankdorfallee 4
3030 Berne

Téléphone 0848 888 888
post@poste.ch
www.poste.ch