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 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 führende Zertifizierungsstellen, die unsere Massnahmen jährlich nach internationalen Sicherheitsstandards prüfen und bewerten.

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 Broschüre 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 oder Ihren Kundenberater.

Informationssicherheit – häufigste Bedrohungen und Gegenmassnahmen

Informationen sind wertvoll. Deshalb müssen wir sie vor kriminellen Angreifern schützen. Kriminelle 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 zunehmend verbreitet. Es setzt entsprechende technische Kenntnisse oder die entsprechenden professionellen Werkzeuge voraus. Darüber hinaus muss der Angreifer Zugang zu einem Hehler-Netzwerk haben, um die Daten verkaufen zu können.

Gegenmassnahmen: Systeme in den Rechenzentren der Post sowie in den von der Post genutzten Cloud-Umgebungen sind durch mehrere Schutzebenen geschützt und stehen unter permanenter Überwachung. Die Post sucht kontinuierlich nach Schwachstellen, 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 auch 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: Solche Praktiken sind weit verbreitet und setzen 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 ungewöhnlich formulierten Aufforderungen oder durch Auffälligkeiten bei Transaktionen 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, so dass 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 vertieftes 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 Online-Dienstleistungen, bis diese überlastet und aus dem Internet nicht mehr zu erreichen sind (sog. Denial-of-Service-Attacken). 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 vertiefte technische Kenntnisse und eine starke Infrastruktur auf Seiten des Angreifers 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:
– Sichern Sie Ihre Daten auf unabhängigen Medien
– Verwenden Sie starke Passwörter und soweit möglich eine Zwei-Faktor-Authentisierung
– Stellen Sie sicher, dass sich Ihre Software auf dem aktuellsten Stand befindet (letzte Updates installiert)
– Schützen Sie Ihre Netzwerk- und Internetverbindung
– Lassen Sie bei dubiosen E-Mails und Anfragen Vorsicht walten
– Sensibilisieren Sie Ihre Mitarbeitenden

Aktuelle Informationen rund um die Informationssicherheit finden Sie auch auf den offiziellen Webseiten spezialisierter Organisationen. Die folgenden können wir Ihnen empfehlen:
– Nationales Zentrum für Cybersicherheit NCSC (früher MELANI) – www.ncsc.admin.ch
– Swiss Cyber Experts – www.swiss-cyber-experts.ch
– Digitalswitzerland – www.digitalswitzerland.com
– Sicheres elektronisches Banking – 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 grösster 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 seit mehreren Jahren 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
Internationale Norm für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheits-Managementsystems (ISMS).

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

ISO 20000-1
International anerkannter Standard für Service-Management in der Informatik.

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 bezieht sich auf die physische Infrastruktur eines Rechenzentrums (Standort, Baukonstruktion, Sicherheitstechnik, Energieversorgung und Kältetechnik) und die organisatorischen Prozesse des Betreibers.

ISAE 3402
PostFinance wird 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.

Meine Sendungen
Komfortables Steuern von Postsendungen nach individuellen Kundenwünschen

Produktbeschreibung

Mit «Meine Sendungen» können Privatkundinnen und -kunden der Post den Empfang ihrer Sendungen steuern. Die Post informiert im Voraus automatisch über ankommende Pakete und eingeschriebene Briefe. Alle Sendungen werden den Kundinnen und Kunden im Kundencenter in der App oder auf der Homepage der Post unter «Meine Sendungen» angezeigt. Ob einzeln oder mit Dauerauftrag: Kundinnen und Kunden können auf ihre Sendungen noch vor der Zustellung nach ihren Wünschen Einfluss nehmen. Beispielsweise Zollgebühren vorgängig bezahlen, die Sendung umleiten oder einen zweiten Zustellzeitpunkt und -ort festlegen. Auch für verpasste Sendungen sind Optionen wählbar. «Meine Sendungen» bringt mehr Flexibilität und höhere Transparenz beim Sendungsempfang.

Verfügbarkeit

Der Service von «Meine Sendungen» steht den Kundinnen und Kunden rund um die Uhr und jeden Tag zur Verfügung. Sie können von überall immer auf ihre Sendungen Einfluss nehmen. Und dank der permanenten Überwachung der Anwendung werden allfällige Störungen rasch erkannt und behoben.

Vertraulichkeit

Die Post schützt personenbezogene Daten, Sendungsdaten und Rechnungsinhalte vor unautorisiertem Zugriff. So verhält es sich auch im Bereich von «Meine Sendungen»: So haben beispielsweise nur diejenigen Post-Mitarbeitenden Kenntnis der Sendungen, die diese Informationen für ihre Aufgabe benötigen.

Integrität

Kundinnen und Kunden können sich darauf verlassen, dass ihre Daten nur in ihrem eigenen Auftrag geändert werden. Die Post stellt für Anpassungen an den Zustellwünschen ein sicheres Login auf der Website oder in der App zur Verfügung.

Nachvollziehbarkeit

Bis eine Sendung beim Empfänger / bei der Empfängerin ankommt, ist es ein langer Weg. Dabei werden alle Änderungen in der Steuerung der Sendung registriert. So stellt die Post sicher, dass nur Berechtigte solche Änderungen vornehmen können.

2020-072 (InfoSec) 06.2023

Zugriff/Identifikation

Kundinnen und Kunden können den Status einer Sendung mit einer Sendungsnummer ohne Login über die PostApp und die Website post.ch abrufen. Falls sie zusätzliche Details zur Sendung wünschen oder etwas ändern wollen, loggen sie sich mit ihrem persönlichen Namen und Passwort ein. Kundinnen und Kunden können ein solches Login der Post mittels SwissID einfach und sicher anlegen. Für besondere Fälle – wie zum Beispiel die Änderung der Adresse – wird den Kundinnen und Kunden ein Bestätigungscode an die hinterlegte E-Mail-Adresse geschickt. Dieser Code ist ein zusätzliches Sicherheitselement (sogenannte Zwei-Faktor-Authentifizierung). Damit stellt die Post sicher, dass der Änderungsauftrag kein Betrugsversuch ist.

Wie kann sich der Kunde schützen?

Personendaten und damit zusammenhängende Informationen sind besonders schützenswert. Mit dem Login in die sicheren Dienstleistungen der Post – beispielsweise über post.ch oder die PostApp – ist bereits ein solider Grundschutz sichergestellt. Kundinnen und Kunden können die Sicherheit mit starken persönlichen Passwörtern vergrössern. Für einen maximalen Schutz sollten diese mit niemandem geteilt werden. Falls Kundinnen und Kunden den Eindruck haben, dass etwas mit ihren Daten nicht stimmt, so hilft die Post schnell und unkompliziert: Unter post.ch, in der App oder in der nächsten Postfiliale.

2020-072 (InfoSec) 06.2023

Post App

Die wichtigsten Informationen und Dienstleistungen der Post auf einen Klick. Jederzeit und überall.

Produktbeschreibung

Mit der Post App der Schweizerischen Post haben Kundinnen und Kunden rund um die Uhr Zugriff auf die wichtigsten Dienstleistungen und Informationen der Post. Kundinnen und Kunden können die App über ein persönliches Login erreichen. Die Post App umfasst insbesondere folgende Dienstleistungen: Meine Sendungen (bspw. Sendungsverfolgung, Abholungseinladung, pick@home, Post zurückbehalten), Standortsuche, Codescanner und Webstamp-Video. Die Dienstleistungen werden laufend ergänzt und auf die Kundenbedürfnisse angepasst.

Verfügbarkeit

Die Post App kann über die jeweiligen App-Stores von Google und Apple bezogen und auf Android- und iOS-Geräten installiert und verwendet werden. Auf der Seite der Kundschaft ist die Verfügbarkeit der Post App vom mobilen oder stationären Internetzugang und allenfalls von der Leistung des verwendeten mobilen Gerätes abhängig. Die Verfügbarkeit der Post App und der darin angebundenen Dienstleistungen ist generell hoch.

Vertraulichkeit

Die über die offiziellen App-Stores erhältliche Post App weist eine hohe Vertraulichkeit aus, da sie eine Eigenentwicklung der Post ist. Die Verbindungen und der Datenaustausch zwischen App und den angebundenen Dienstleitungen sind verschlüsselt. Sensitive Daten wie Kundenadressen und Sendungsdaten werden nicht lokal auf der App gespeichert. Für die Verwendung geschützter Funktionalitäten innerhalb der Post App benötigen Kundinnen und Kunden eine separate Anmeldung mittels Benutzernamen und Passwort, was die Sicherheit zusätzlich erhöht.

Integrität

Die Verschlüsselung der Verbindungen und des Datenaustausches zwischen App und den angebundenen Dienstleitungen gewährleistet die Integrität der Daten. Darüber hinaus verifiziert die App mittels eines zusätzlichen Sicherheitsmechanismus (Zertifikat) die Herkunft der Daten.

Nachvollziehbarkeit

Ausgeführte Tätigkeiten in den angebundenen Dienstleistungen der Schweizerischen Post werden nachvollziehbar geloggt.

Zugriff/Identifikation

Für die Verwendung geschützter Funktionalitäten innerhalb der Post App ist ein Post-Benutzerkonto mit Benutzername und Passwort notwendig. Die Übertragung der Login-Daten erfolgt verschlüsselt. Die erweiterten Funktionalitäten in der Post App sind mit SwissID-Login geschützt.

2020-072 (InfoSec) 06.2023

Wie kann sich der Kunde schützen?

Kundinnen und Kunden wird geraten, ihr mobiles Gerät mit PIN, Gesichtserkennung oder Fingerabdruck zu sichern. Damit lässt sich im Falle eines Verlusts oder Diebstahls des Geräts verhindern, dass Dritte ungeschützt auf persönliche Informationen der Post App zugreifen können.

Der Bezug der Post App wird ausschliesslich über die offiziellen App-Stores von Android oder Apple empfohlen.

Das nicht autorisierte Entfernen von Nutzungsbeschränkungen des genutzten Gerätes (sogenanntes Jailbreaking) wird nicht empfohlen. Nutzungsbeschränkungen werden von Herstellern aus Sicherheitsgründen bewusst implementiert. Werden diese entfernt, kann es zu unberechtigten Zugriffen auf das Gerät kommen und beispielsweise zu Datendiebstahl oder dem Zugriff auf Banking-Apps führen.

2020-072 (InfoSec) 06.2023

Postshop
Sicher einkaufen auf postshop.
Vielfältige Angebote auf einen Klick.

Produktbeschreibung

Postshop.ch ist der Onlineshop der Post. Er bietet Produkte an, die einen Bezug zum Geschäft der Post aufweisen und die den Alltag der Kundinnen und Kunden leichter machen: von Smartphones über Geschenkkarten bis zu Büro- und Papeterieprodukten. Auch die neuesten Briefmarken der Post sowie passendes Verpackungsmaterial für den Versand von Briefen und Paketen können bequem online bestellt werden. Die Verschlüsselung der Informationen und eine zertifizierte Zahlungsplattform garantieren dabei die Sicherheit beim Einkauf.

Verfügbarkeit

Der Postshop hat eine sehr hohe Verfügbarkeit: Er funktioniert rund um die Uhr mit minimalen Ausfallzeiten. Die Post führt periodische Lastentests durch und überprüft mit einem aktiven Monitoring, ob die definierten Zielwerte eingehalten werden.

Vertraulichkeit

Die Post stellt sicher, dass die Daten im Onlineshop nur von den Personen eingesehen oder offengelegt werden dürfen, die dazu auch berechtigt sind. Die Post analysiert periodisch den Schutzbedarf und ihr Berechtigungskonzept für den Onlineshop. Sie geht umsichtig mit den Daten im Postshop um und setzt die Vorgaben aus Datenschutz und Gesetzen um.

Integrität

Die Post überprüft und optimiert ihren Onlineshop laufend. Vor jedem grossen Update lässt sie von einer unabhängigen Stelle Sicherheitstests durchführen, die sich an internationalen Standards orientieren (OWASP Top 10). Zudem ist der Postshop im Bug-Bounty-Programm der Post vertreten, bei dem ethische Hacker im Auftrag der Post Sicherheitslücken suchen. Allfällig identifizierte Schwachstellen korrigiert die Post umgehend.

Nachvollziehbarkeit

Eine Überwachung (Monitoring) stellt sicher, dass Dritte keine Kundendaten im Postshop unbemerkt verändern können.

Zugriff/Identifikation

Wer im Postshop einkaufen möchte, kann sich mit SwissID anmelden oder auch als Gast bestellen. Auf Rechnung einkaufen und Gutscheine einlösen können jedoch nur Brief-registrierte Kundinnen und Kunden. Einzelne Waren wie Geschenkkarten und E-Gutscheine müssen in jedem Fall sofort bezahlt werden. Diese Massnahmen erhöhen die Hürde für allfällige Betrugsversuche.

2020-072 (InfoSec) 06.2023

Wie kann sich der Kunde schützen?

Der sorgsame Umgang mit dem SwissID-Passwort sowie mit den Daten der Post-, Bank- oder Kreditkarte bildet die Basis der Sicherheit. Das Passwort sollte schwierig zu erraten sein und ausschliesslich für die SwissID verwendet werden. Um die Sicherheit zusätzlich zu erhöhen, loggen sich Kundinnen und Kunden optimalerweise direkt im Postportal ein. Dies ist sicherer, als einem Link in einer (unerwarteten) E-Mail zu folgen, da dies ein Phishing-Versuch sein kann.

2020-072 (InfoSec) 06.2023

Verzollung von Waren und Sendungen

Sichere Verfahren im Import und Export von Waren und Sendungen garantieren eine zügige Abwicklung, eine schnelle Zustellung und zugleich einen sicheren Umgang mit schützenswerten Daten.

Produktbeschreibung

Nahezu alle Postbetreiber sind im Weltpostverein UPU verbunden und folgen dessen Vorgaben auch hinsichtlich Lieferbedingungen und Abrechnungsthemen; so auch die Schweizerische Post. Zu den normalen Postdienstleistungen kommen zoll- und steuerrechtliche Aufgaben hinzu. Hier ist die Schweizerische Post verpflichtet, die relevanten Dokumente zu erstellen bzw. einzuholen, um eine Deklaration zur Verzollung durchführen zu können. Anhand der Angaben zur Sendung wird der Wert und damit auch die Höhe der zu entrichtenden Zollgebühr festgelegt. Auch dieser Prozess wird weiterentwickelt und zunehmend digitaler.

Verfügbarkeit

Kundinnen und Kunden können die für die Deklaration nötigen Informationen über die Sendung (bspw. Inhalt, Gewicht und Wert) am Schalter oder digital (bspw. über das Benutzerkonto auf post.ch oder über die Post App) erfassen. Durch die digitalen Möglichkeiten sind Kundinnen und Kunden nicht mehr an Orte oder Öffnungszeiten gebunden und können die Eintragungen flexibel vornehmen. Einfach wenn es ihnen am besten passt – auch von zu Hause aus.

Vertraulichkeit

Die Post schützt personenbezogene Daten, Sendungsdaten und Rechnungsinhalte vor unautorisiertem Zugriff. Sie verarbeitet Kundendaten und stellt diese in der Verzollung auch den Zollbehörden bereit, wozu sie verpflichtet ist. Im Rahmen der Sendungsverfolgung oder in der Rechnungsstellung ist der sichere Datenaustausch zwischen Kundschaft und Post unverzichtbar. Kunden-Logins, geprüfte Websites und verschlüsselte Verbindungen zu externen Partnern stellen dies sicher.

Integrität

Kundinnen und Kunden haben Anspruch, dass ihre Daten nur von der Post und nur in begründeten Fällen geändert werden dürfen. Dies ist beispielsweise dann der Fall, wenn Anpassungen im Namen, in der Adresse oder in den Kontodaten vorgenommen werden müssen. Während der ganzen Verarbeitung sind die Daten geschützt und sicher.

Nachvollziehbarkeit

Bis die Sendung beim Empfänger zu Hause ankommt, ist es ein langer Weg – gerade im Import und Export. In jedem Verarbeitungsschritt wird die Sendung gescannt. Gerade im Bereich der Verzollung ist die damit gewährleistete Nachvollziehbarkeit ein wesentlicher Faktor, damit die Sendung korrekt transportiert und die Zollgebühren korrekt berechnet werden können.

2020-072 (InfoSec) 06.2023

Zugriff/Identifikation

Die Post erweitert laufend ihre physischen und digitalen Kontaktpunkte. Dabei muss die Post die Identität ihrer Kundinnen und Kunden sicherstellen. Nur so kann die Post mit ihren Kundinnen und Kunden über wichtige Inhalte wie beispielsweise die Sendung sprechen oder ihnen schützenswerte und nur für sie bestimmte Informationen zukommen lassen. Das kann durch ein Kunden-Login auf post.ch erfolgen oder durch die Vorlage des entsprechenden Ausweises in der Filiale. Die Identifikation ist der Schlüssel für den Zugang zu unseren Dienstleistungen und den damit zusammenhängenden Daten.

Wie kann sich der Kunde schützen?

Betrüger versuchen, über Phishing an Kreditkartendetails von Dritten zu gelangen. Oft tun sie dies, indem sie diese zur Bezahlung einer ausstehenden Rechnung auffordern. Dies könnte auch im Bereich der Sendungsdaten geschehen. Die Post bittet um besondere Vorsicht. Wenn betroffene Kundinnen oder Kunden keine Sendung bei der Post aufgegeben haben oder auch keine Bestellung erwarten, sollen diese Phishing-E-Mails ignoriert werden. Wenn doch eine Sendung aufgegeben wurde oder eine erwartet wird, dann kann die Rechnung am besten im Benutzerkonto der Post eingesehen werden. Alternativ können sich Kundinnen und Kunden an die nächste Poststelle wenden. So sind sie sicher, dass die Rechnung von der Post kommt und damit ordnungsgemäss ist.

Sollte etwas rund um Brief- und Paketsendungen ungewöhnlich erscheinen, so stehen unsere Poststellen oder unser Contact Center mit Rat zur Seite. Falls Kundinnen und Kunden nicht sicher sind, ob sie doch zu schnell auf eine E-Mail geklickt haben, empfiehlt sich eine sofortige Passwortänderung oder die Verwendung der Zwei-Faktor-Authentifizierung.

2020-072 (InfoSec) 06.2023

Zustelldienstleistungen
Praktisch und sicher

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

Produktbeschreibung

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.

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.

2020-072 (InfoSec) 06.2023

2020-072 (InfoSec) 06.2023

Post CH AG
Wankdorfallee 4
3030 Bern

Telefon 0848 888 888
post@post.ch
www.post.ch