Sicurezza delle informazioni della Posta

In tutta tranquillità

Prefazione

Marcel Zumbühl
CISO, la Posta

Gentile cliente,

la sicurezza delle informazioni non è semplicemente un tema di carattere tecnico. Anche le tecnologie migliori, infatti, possono rivelarsi inutili se manca l'aspetto più importante: la fiducia. Per la Posta è fondamentale trasmetterle questo sentimento di fiducia e fornirle consulenza e supporto per tutte le questioni riguardanti la sicurezza delle informazioni.

Per noi la sicurezza dei suoi dati è un aspetto a cui dedicare la massima attenzione. Un'attenzione che inizia fin dalla fase di sviluppo di un'offerta, ovvero molto prima che i nostri clienti possano iniziare a utilizzare i nostri prodotti e servizi. E, naturalmente, garantiamo che i vostri dati vengano protetti adeguatamente e rimangano al sicuro durante l'esercizio. Sottoponiamo ad esempio i nostri prodotti a test regolari e nei nostri centri di calcolo ne monitoriamo il funzio namento 24 ore su 24. In questo modo siamo in grado di riconoscere precocemente possibili tentativi di attacco da parte di hacker per mettere in campo contromisure adeguate.

Ci mettiamo inoltre regolarmente alla prova confrontandoci con rinomati esperti ed esperte esterni. Così siamo in grado di comprendere come e dove è possibile migliorare ulteriormente la sicurezza per i nostri clienti. Nel campo della sicurezza non ci si ferma mai. L'elevata qualità con cui la Posta gestisce la sicurezza delle informazioni è confermata anche da certificatori indipendenti, che ogni anno verificano le nostre misure e ne dichiarano la conformità agli standard di sicurezza internazionali.

Tutte le misure di sicurezza che implementiamo sono ovviamente attive in background e hanno un unico obiettivo: contribuire al successo dei nostri clienti garantendo un esercizio ottimale e affidabile dei nostri prodotti e servizi, affinché possano sempre sentirsi al sicuro.

Cordiali saluti
Marcel Zumbühl, CISO, la Posta

Sicurezza delle informazioni della Posta

Questa cartellina contiene diversi factsheet sul tema della sicurezza delle informazioni dei nostri principali prodotti e servizi. Le informazioni in essi pubblicate vengono regolarmente verificate e aggiornate in stretta collaborazione con la Gestione prodotti, i responsabili della sicurezza, la Comunicazione e il Servizio legale della Posta. Per maggiori informazioni è possibile rivolgersi al proprio consulente clienti o a Sicurezza dell'informazione della Posta.

Sicurezza delle informazioni: le minacce più frequenti e le contromisure possibili

Le informazioni sono preziose. Per questo motivo devono essere protette da chi cerca di impadronirsene con intenti criminali, sfruttandone le vulnerabilità al fine di procurarsi vantaggi illegittimi. Gli attacchi più comuni sono, quindi, il furto di informazioni, il phishing e l'abuso di identità, la distruzione e la manipolazione di informazioni e gli attacchi DDoS contro i centri di calcolo.

Furto di informazioni

Procedura: i criminali entrano nei sistemi informatici, sottraggono informazioni e le vendono sul mercato nero. Gli obiettivi preferiti di questi delinquenti sono: informazioni personali, dati aziendali, dati delle carte di credito e in generale informazioni sui processi finanziari. Spesso i criminali, fornendo false identità, cercano di ottenere la fiducia della vittima per arrivare esattamente dove vogliono.

Valutazione: questo modello di attacco è largamente diffuso. Richiede elevate conoscenze tecniche oppure presuppone l'impiego di adeguati strumenti professionali. Inoltre queste persone devono avere accesso a una rete di ricettatori per riuscire a vendere i dati.

Contromisure: i sistemi nei centri di calcolo della Posta sono protetti da più livelli di sicurezza e sono oggetto di una sorveglianza costante. Gli esperti sono sempre alla ricerca di possibili punti deboli, allo scopo di eliminarli o circoscriverli adottando misure aggiuntive.

Phishing e furto di identità

Procedura: i criminali carpiscono la fiducia della vittima falsificando e-mail, messaggi di testo o addirittura telefonate per poi assumerne l'identità digitale. Possono anche acquistare l'identità delle vittime (ad es. dati di accesso agli account) sul mercato nero e utilizzano l'identità sottratta per cercare di ordinare merce, manipolare servizi o rubare direttamente denaro dai i conti bancari.

Valutazione: metodo molto diffuso e che non richiede elevate conoscenze tecniche. Generalmente questo tipo di attacco avviene a ondate.

Contromisure: per contrastare i furti di identità e il phishing è molto importante che sia i clienti sia la Posta siano sempre estremamente vigili e abbiano prontezza di riflessi. È possibile smascherare e bloccare gli attacchi poiché spesso i testi e il linguaggio presentano lievi irregolarità oppure poiché il comportamento dei sistemi presenta anomalie.

Manipolazione dei dati e perdita di informazioni

Procedura: i criminali entrano nei sistemi, creano una copia delle informazioni e distruggono l'originale oppure lo crittografano fino al punto da renderlo inaccessibile. Successivamente ricattano la vittima utilizzando l'informazione o i mezzi di accesso ai dati come cauzione.

Valutazione: generalmente questi attacchi vengono utilizzati in maniera mirata. Richiedono approfondite conoscenze tecniche e informazioni dettagliate sulla vittima.

Contromisure: per difendersi da questi attacchi la Posta si avvale di innumerevoli meccanismi di protezione. Inoltre collabora a stretto contatto con le autorità di perseguimento penale. In questo modo è possibile reagire con risolutezza a un tentativo di attacco.

Attacchi DDoS contro le infrastrutture

Procedura: i criminali attaccano in maniera mirata l'accesso ai servizi finché il sistema non si sovraccarica e non è più raggiungibile da internet. Successivamente ricattano la vittima pretendendo denaro in cambio della risoluzione della situazione di sovraccarico.

Valutazione: questi attacchi sono sporadici e generalmente sono tentativi volti a sondare l'efficacia dei meccanismi di protezione. Presuppongono approfondite conoscenze tecniche e un'infrastruttura performante dedicata.

Contromisure: la Posta, in collaborazione con i gestore di rete, si dota di meccanismi di difesa, regolarmente sottoposti a verifiche, che le consentono di difendersi dagli attacchi DDoS.

Che cosa potete fare per proteggervi

Le regole fondamentali per aumentare la sicurezza:
- utilizzate password complesse
- eseguite regolarmente gli aggiornamenti
- proteggete il collegamento di rete e la connessione a internet
- crittografate i vostri dati
- prestate attenzione nel caso di e-mail e richieste sospette

Informazioni attuali sulla sicurezza delle informazioni sono disponibili anche sui siti web ufficiali di organizzazioni specializzate. Vi consigliamo le seguenti:

- Centro nazionale per la cibersicurezza NCSC (in precedenza MELANI) – www.ncsc.admin.ch
- Swiss Cyber Experts – www.swiss-cyber-experts.ch
- ICT Switzerland – www.ictswitzerland.ch
- ebas.ch – www.ebas.ch

Protezione dei dati

Nella fornitura di prestazioni ai suoi clienti, la Posta ritiene imprescindibile garantire una gestione dei dati personali responsabile e a norma di legge.

Per questo la Posta gestisce i dati personali con la massima diligenza e in conformità alle leggi vigenti in materia di protezione dei dati e alla legislazione postale.

La Posta dispone di un sistema completo di protezione dei dati, in base al quale verifica la conformità di ogni servizio fornito.

Sicurezza certificata

Per le tematiche fondamentali in materia di sicurezza, la Posta è certificata ai sensi di standard riconosciuti a livello internazionale. Si attiene pertanto alle relative best practice e semplifica i processi di compliance dei clienti. Ecco alcuni degli standard.

ISO 27001
La norma internazionale stabilisce i requisiti per l'allestimento, l'attuazione, il mantenimento e il miglioramento continuo di un sistema di gestione della sicurezza delle informazioni (ISMS).

ISO 22301
La norma internazionale specifica i requisiti per avviare e gestire un sistema efficace di Business Continuity Management (BCMS).

TÜV Trusted Site Infrastructure TSI V3.2 Dual Site Level 3
Entrambi i centri di calcolo della Posta si trovano in Svizzera e in località geograficamente indipendenti. Offrono un ambiente di hosting di prima categoria caratterizzato da più livelli di sicurezza. La certificazione definisce i requisiti dell'infrastruttura fisica di un centro di calcolo (sede, costruzione dell'edificio, tecnica di sicurezza, approvvigionamento energetico e refrigerazione) e i processi organizzativi del gestore. Inoltre documenta l'idoneità delle aree di sicurezza, per le quali è richiesta un'elevata disponibilità.

ISAE 3402
L'efficacia dei controlli del sistema di controllo interno dell'istituto finanziario PostFinance e di Swiss Post Solutions, service provider per istituti finanziari, viene verificata e certificata in collaborazione con l'unità Informatica della Posta in conformità all'International Standard on Assurance Engagements (ISAE) 3402.

PCI DSS
Il Payment Card Industry Data Security Standard (PCI DSS) è stato sviluppato dal PCI Security Standards Council per limitare le truffe nei pagamenti online con carta di credito.

Postshop
Acquisti sicuri nello shop online della Posta

Su postshop.ch possono essere ordinate con un semplice clic molte offerte che facilitano la vita quotidiana. Al momento dell'acquisto la sicurezza è garantita dalla codifica delle informazioni e da una piattaforma di pagamento certificata.

Diverse modalità di accesso al portale

Chi desidera acquistare su Postshop può registrarsi tramite Login clienti Posta o con SwissID oppure ordinare come utente ospite. Le funzioni di pagamento delle fatture e riscossione dei buoni possono invece essere utilizzate solo da clienti registrati. Inoltre le carte regalo e i buoni elettronici non possono essere acquistati contro fattura. Queste misure sono volte a ostacolare eventuali tentativi di frode.

Elevata disponibilità

Nel primo semestre del 2020 Postshop ha registrato un tasso di disponibilità del 99,5%. Per riuscire a far fronte a volumi ancora maggiori, la Posta esegue periodicamente test di carico. Inoltre, tramite un monitoraggio attivo ne valuta la disponibilità e verifica se i benchmark definiti vengono rispettati.

Sistema di pagamento sicuro

I dati dei clienti Postshop vengonosalvati esclusivamente in Svizzera. Chi paga con la carta di credito viene indirizzato dal Postshop a BillingOnline, la piattaforma di pagamento sicura della Posta, certificata secondo lo standard di sicurezza PCI DSS. Questa norma di sicurezza internazionale protegge i dati degli utenti dal furto digitale e da utilizzi illeciti. Tutto il traffico di rete su internet è cifrato.

Test completi

La Posta verifica e ottimizza costantemente Postshop. Da un lato Postshop rientra tra i programmi bug bounty della Posta e, pertanto, è possibile correggere tempestivamente eventuali punti deboli individuati (finding). Dall'altro la Posta sottopone regolarmente i propri calcolatori e le reti a un test di sicurezza completo, basato su standard internazionali (OWASP Top 10). La Posta analizza inoltre periodicamente il fabbisogno di protezione e il piano di sicurezza dell'informazione e, prima di ogni aggiornamento di rilievo del Postshop, richiede l'esecuzione di test di sicurezza da parte di un ufficio di verifica indipendente.

Che cos'è Postshop?
Il Postshop è lo shop online della Posta e offre prodotti e servizi che presentano un'attinenza con l'azienda: dagli smartphone alle carte regalo fino agli accessori da viaggio. Basta un semplice clic per ordinare i francobolli più recenti della Posta oppure il materiale d'imballaggio per spedire lettere e pacchi. www.postshop.ch

2020-072 (InfoSec) 05.2021

Posta CH SA
Wankdorfallee 4
3030 Berna

N. tel. 0848 888 888
E-mail post@posta.ch
www.posta.ch

LA POSTA

Prestazioni di recapito
Pratiche e sicure

Con le sue prestazioni di recapito, la Posta offre a clienti privati e commerciali innumerevoli possibilità per gestire la ricezione degli invii in tutta comodità.

Identificazione personale

Le prestazioni di recapito della Posta sono a disposizione di tutti i clienti. Per utilizzare tali prestazioni è obbligatoria un'identificazione personale. I clienti commerciali devono inoltre presentare un documento probatorio, ad esempio un estratto RC o gli statuti dell'associazione. La Posta conferma soltanto di aver preso visione dei documenti d'identificazione, non trattiene i documenti e non li salva.

Flusso di dati completamente automatizzato

I dati acquisiti nell'ambito di queste prestazioni vengono trasmessi con modalità completamente automatizzate tramite un'applicazione centrale della Posta. In questo modo si garantisce che tutte le prestazioni interessate dispongano sempre di dati attuali. I dati restano sempre presso la Posta.

Accesso rigorosamente regolamentato

Alle prestazioni di recapito o all'applicazione centrale, che salva i dati necessari per i servizi, hanno accesso soltanto i collaboratori della Posta con diritti utente specifici. Se un utente è inattivo per 90 giorni, la sua autorizzazione viene automaticamente cancellata.

Imparare a proteggersi

I clienti possono aumentare il proprio livello di protezione scegliendo una password il più possibile sicura per il Login clienti Posta ed evitando di salvarla nel browser o di condividerla con altri.

Che cosa sono le prestazioni di recapito?
Avviare e gestire ordini di rispedizione, modificare indirizzi e comunicare traslochi. Questi sono solo alcuni esempi delle innumerevoli prestazioni di recapito che la Posta offre ai propri clienti. Le prestazioni di recapito possono essere utilizzate 24 ore su 24 online (PC, smartphone, tablet) tramite il Login clienti Posta, durante gli orari di apertura degli sportelli oppure tramite il servizio clienti. www.posta.ch/ricezione

2020-072 (InfoSec) 05.2021

Posta CH SA
Wankdorfallee 4
3030 Berna

N. tel. 0848 888 888
E-mail post@posta.ch
www.posta.ch

LA POSTA

PubliBike
Viaggiare sicuri

PubliBike consente di noleggiare biciclette tradizionali e e-bike in tutta la Svizzera. Per registrarsi al servizio è necessario effettuare il login, il costo viene conteggiato in base ai minuti di noleggio e il pagamento viene effettuato tramite carta di credito. La Posta assicura che il servizio sia e rimanga sicuro.

La ridondanza garantisce la disponibilità

I dati di PubliBike vengono salvati in due centri di calcolo certificati ai sensi della norma ISO 27001. In caso di mancato funzionamento di uno dei due centri, la ridondanza assicura che i dati e il funzionamento di PubliBike siano garantiti. Le interazioni con i clienti avvengono su server diversi, al fine di evitare un grado di utilizzo eccessivo di un singolo server.

Gestione confidenziale dei dati

La protezione dei dati personali degli utenti è di estrema importanza per la Posta. Per questo gestisce questi dati personali con la massima diligenza e in conformità alle leggi vigenti in materia di protezione dei dati e alle altre norme di legge. L'intero traffico di dati su internet è cifrato.

Misure di sicurezza

Un sistema di riconoscimento degli attacchi consente di individuare, analizzare e impedire immediatamente eventuali modifiche non autorizzate dei sistemi di PubliBike. Inoltre viene regolarmente verificata la presenza di punti deboli nei sistemi, ad esempio mediante un test di sicurezza completo basato su standard internazionali (OWASP Top 10). L'utilizzo delle componenti di sistema viene registrato in un logbook al fine di garantire il tracciamento e viene verificata la presenza di eventuali irregolarità.

Che cos'è PubliBike?
PubliBike è l'offerta di bike sharing più grande della Svizzera. Questo servizio è il completamento ideale dei mezzi di trasporto pubblici e privati per gli spostamenti a breve distanza, contribuisce alla riduzione del traffico e promuove la salute degli utenti. PubliBike è la soluzione ideale anche per unire le diverse sedi, ad es. di università, amministrazioni o grandi aziende. www.publibike.ch

2020-072 (InfoSec) 05.2021

Posta CH SA
Wankdorfallee 4
3030 Berna

N. tel. 0848 888 888
E-mail post@posta.ch
www.posta.ch

LA POSTA

Document Input Processing
Scansione e preparazione dei documenti in sicurezza

Con Document Input Processing (DIP) Swiss Post Solutions elabora dati non strutturati da documenti fisici ed elettronici in entrata per i clienti commerciali. La protezione dei dati è sempre garantita.

Elevata disponibilità

Swiss Post Solutions (SPS) garantisce la massima disponibilità del servizio grazie all'attuazione di svariate misure tra cui rientrano, ad esempio, un'infrastruttura dei centri di calcolo basata sul mirroring, test regolari di ripristino e backup della banca dati nonché una connessione di rete ridondante per le sedi grazie ai cosiddetti meccanismi di failover. Queste soluzioni assicurano, in caso di avaria di un calcolatore, il subentro diretto del secondo calcolatore nello svolgimento dei compiti del primo.

Codifica end-to-end

Lo scambio di dati con clienti che utilizzano DIP mediante Document Input Processing (DIP) è sempre cifrato e si svolge tramite Secure File Transfer Protocol (SFTP) e/o Virtual Private Network Tunnel (VPN). Le reti sono inoltre protette da firewall.

Misure di sicurezza tecniche

All'interno della rete protetta di SPS, DIP funziona tramite un local area network dedicato (VLAN). È possibile accedere alla rete VLAN solo mediante un'autenticazione a più fattori. Per analizzare i file di log in tempo reale e rintracciare tutte le transazioni viene utilizzato un sistema di log monitoring. Grazie al monitoraggio attivo della rete, i possibili attacchi informatici vengono tempestivamente identificati e respinti.

Misure di sicurezza fisiche

Solo i collaboratori di SPS in possesso di un apposito badge hanno accesso ai locali di produzione di DIP. I collaboratori sono soggetti all'obbligo di segretezza e al segreto postale. Gli accessi sono protocollati e l'edificio è videosorvegliato. Prima di ricevere diritti utente estesi, i collaboratori vengono inoltre sottoposti a una procedura di test (screening).

Standard di sicurezza internazionali

Per l'utilizzo di DIP si applicano disposizioni di servizio esaustive in materia di sicurezza, come ad esempio la norma ISO 27001 sulla sicurezza delle informazioni, in Svizzera il Payment Card Industry Data Security Standard (PCI DSS) per le transazioni con carta di credito e negli USA l'Health Insurance Portability and Accountability Act (HIPAA) per la tutela delle informazioni sanitarie. Il rispetto di questi standard viene verificato regolarmente.

Che cos'è Document Input Processing?
Con Document Input Processing (DIP) Swiss Post Solutions ottimizza i processi aziendali basati su documenti. I processi di elaborazione sono altamente standardizzati e vengono sistematicamente perfezionati e migliorati. Tra questi rientrano l'accettazione e la preparazione dei documenti, la loro scansione, indicizzazione, elaborazione e archiviazione. DIP offre, pertanto, tutte le soluzioni necessarie per preparare automaticamente dati non strutturati e metterli a disposizione dei clienti.
www.swisspostsolutions.com/dip

2020-072 (InfoSec) 05.2021

Posta CH SA
Wankdorfallee 4
3030 Berna

N. tel. 0848 888 888
E-mail post@posta.ch
www.posta.ch

LA POSTA

Document Output Processing
Gestione output sicura per clienti commerciali

Con il Document Output Processing, Swiss Post Solutions gestisce per i clienti commerciali la preparazione dei dati, la stampa e l'invio dei documenti relativi alle transazioni. La protezione dei dati è sempre garantita.

Elevata disponibilità

Document Output Processing (DOP) di Swiss Post Solutions (SPS) gestisce nei grandi centri lettere i siti di produzione per la preparazione dei dati, la stampa e l'invio di documenti. Oltre a diverse procedure di sicurezza e ripristino, nei siti di produzione è inoltre previsto un esercizio di emergenza che garantisce la disponibilità in caso di eventi straordinari.

Codifica end-to-end

Lo scambio di dati con i clienti che utilizzano DOP è cifrato e si svolge tramite Secure File Transfer Protocol (SFTP) e/o Virtual Private Network (VPN) Tunnel. Le reti sono inoltre protette da firewall.

Misure di sicurezza tecniche

All'interno della rete protetta di SPS, DIP funziona tramite un local area network dedicato (VLAN). È possibile accedere alla rete VLAN solo mediante un'autenticazione a più fattori. Per l'analisi dei file di log viene impiegato un sistema di log monitoring completo. Inoltre tutte le transazioni sono rintracciabili e salvate in maniera incontestabile. Partner esterni certificati garantiscono un processo di distruzione dei supporti di memoria standardizzato.

Misure di sicurezza fisiche

Solo i collaboratori di SPS in possesso di un apposito badge hanno accesso ai locali di produzione di DOP. I collaboratori sono soggetti all'obbligo di segretezza e al segreto postale. Gli accessi sono protocollati e l'edificio è videosorvegliato. Prima di ricevere diritti utente estesi, i collaboratori vengono inoltre sottoposti a una procedura di test (screening).

Standard di sicurezza internazionali

Per l'utilizzo di DOP si applicano disposizioni di servizio esaustive in materia di sicurezza, come ad esempio la norma ISO 27001 sulla sicurezza delle informazioni, in Svizzera il Payment Card Industry Data Security Standard (PCI DSS) per le transazioni con carta di credito e negli USA l'Health Insurance Portability and Accountability Act (HIPAA) per la tutela delle informazioni sanitarie. Il rispetto di questi standard viene verificato regolarmente.

Che cos'è Document Output Processing?
Con Document Output Processing Swiss Post Solutions gestisce per i clienti commerciali la stampa e il recapito di documenti commerciali relativi alle transazioni, come fatture, polizze o estratti conto. I documenti possono essere trasmessi ai clienti finali tramite canali fisici, digitali o con un mix di entrambi. La gestione output automatizzata consente di risparmiare risorse e garantisce al contempo stabilità, sicurezza e redditività. www.swisspostsolutions.com/dop

2020-072 (InfoSec) 05.2021

Posta CH SA
Wankdorfallee 4
3030 Berna

N. tel. 0848 888 888
E-mail post@posta.ch
www.posta.ch

LA POSTA

2020-072 (InfoSec) 05.2021

Posta CH SA
Wankdorfallee 4
3030 Berna

N. tel. 0848 888 888
E-mail post@posta.ch
www.posta.ch