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 dimostrarle di essere un partner affidabile 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 suoi dati vengano protetti 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 funzionamento 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 enti di certificazione leader indipendenti, che ogni anno verificano le nostre misure e ne valutano 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

Questo opuscolo contiene diversi factsheet sul tema della sicurezza delle informazioni dei nostri principali prodotti e servizi. Le informazioni pubblicate al suo interno vengono regolarmente verificate e aggiornate in stretta collaborazione con la Gestione prodotti, i responsabili sicurezza, la Comunicazione e il Servizio legale della Posta. In caso di domande è possibile rivolgersii al proprio o alla propria consulente clienti.

Sicurezza delle informazioni: le minacce più frequenti e le contromisure

Le informazioni sono preziose. Per questo motivo dobbiamo proteggerle da chi cerca di impadronirsene con intenti criminali, sfruttandone le vulnerabilità al fine di procurarsi vantaggi illegittimi. Gli attacchi più comuni sono 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

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

Analisi: questo modello di attacco è largamente diffuso. Richiede conoscenze tecniche specifiche oppure presuppone l'impiego di strumenti professionali adatti. Inoltre, chi lo perpetra deve disporre di una rete di ricettatori per riuscire a vendere i dati.

Contromisure: i sistemi nei centri di calcolo della Posta e negli ambienti cloud utilizzati dalla Posta sono protetti da più livelli di sicurezza e sono monitorati continuamente. La Posta è sempre alla ricerca di possibili punti deboli, allo scopo di eliminarli o circoscriverli adottando misure aggiuntive.

Phishing e furto di identità

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

Analisi: sono pratiche molto diffuse che non richiedono conoscenze tecniche approfondite. 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 reagiscano immediatamente. Gli attacchi si possono riconoscere dalle richieste insolite o da anomalie nelle transazioni, e quindi essere bloccati.

Manipolazione dei dati e perdita di informazioni

Come funziona: 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.

Analisi: 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

Come funziona: i criminali attaccano in maniera mirata i servizi online finché il sistema non si sovraccarica e non è più raggiungibile da internet (si parla infatti di attacchi denial-of-service). Successivamente ricattano la vittima pretendendo denaro in cambio della risoluzione della situazione di sovraccarico.

Analisi: si tratta soprattutto di tentativi sporadici volti a sondare l'efficacia dei meccanismi di protezione. Questi attacchi presuppongono conoscenze tecniche approfondite e una solida infrastruttura da parte di chi li perpetra.

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

Che cosa si può fare per proteggersi

Le regole fondamentali per aumentare la sicurezza sono:
– salvare i dati su supporti indipendenti
– utilizzare password sicure e, ove possibile, l'autenticazione a due fattori
– Assicurarsi di utilizzare la versione più recente del software (cioè di aver installato l'ultimo aggiornamento)
– Proteggere il collegamento di rete e a internet
– Fare attenzione in caso di e-mail e richieste dubbiose
– Sensibilizzare il personale

Informazioni attuali sulla sicurezza delle informazioni sono disponibili anche sui siti web ufficiali di organizzazioni specializzate. Consigliamo i seguenti:
– Centro nazionale per la cibersicurezza NCSC (in precedenza MELANI) www.ncsc.admin.ch
– Swiss Cyber Experts www.swiss-cyber-experts.ch
– Digitalswitzerland – www.digitalswitzerland.com
– eBanking sicuro 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 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 da molti anni 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
Norma internazionale per l'allestimento, l'attuazione, il mantenimento e il miglioramento continuo di un sistema di gestione della sicurezza delle informazioni (ISMS).

ISO 22301
Norma internazionale per la creazione e la gestione di un efficace Business Continuity Management System (BCMS).

ISO 20000-1
Standard riconosciuto a livello internazionale per la gestione dei servizi a livello informatico.

TÜV Trusted Site Infrastructure TSI V3.2 Dual Site Level 3
Entrambi i centri di calcolo della Posta si trovano in Svizzera in località geograficamente indipendenti. Offrono un ambiente di hosting di prima categoria caratterizzato da più livelli di sicurezza. La certificazione riguarda l'infrastruttura fisica di un centro di calcolo (sede, costruzione dell'edificio, tecnica di sicurezza, approvvigionamento energetico e refrigerazione) e i processi organizzativi del gestore.

ISAE 3402
L'efficacia del sistema di controllo interno di PostFinance 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.

I miei invii

Gestire gli invii postali in modo pratico in base alle esigenze della clientela

Descrizione del prodotto

Con «I miei invii» la clientela privata della Posta può gestire la ricezione dei propri invii. La Posta invia in anticipo notifiche automatiche sui pacchi e sulle lettere raccomandate in arrivo. Tutti gli invii possono essere consultati nel centro clienti disponibile nell'app o sulla homepage della Posta sotto «I miei invii». Che si tratti di un singolo ordine o di un ordine permanente, le e i clienti possono gestire gli invii in base alle proprie esigenze, prima del loro recapito. È possibile, ad esempio, pagare anticipatamente le spese doganali, rispedire un invio, scegliere un secondo momento e un secondo luogo del recapito, nonché selezionare opzioni di gestione per gli invii mancati. «I miei invii» offre maggiore flessibilità e trasparenza a livello di ricezione degli invii.

Disponibilità

Il servizio «I miei invii» è disponibile 24 ore su 24, 7 giorni su 7, permettendo alla clientela di gestire i propri invii ovunque e in qualsiasi momento. Inoltre, grazie al sistema di sorveglianza permanente dell'applicazione è possibile rilevare e risolvere rapidamente eventuali guasti.

Riservatezza

La Posta protegge i dati personali, i dati dell'invio e i contenuti della fattura da accessi non autorizzati. Lo stesso principio si applica anche a «I miei invii»: ad esempio, solamente i membri del personale della Posta che hanno bisogno di queste informazioni per lo svolgimento del proprio lavoro, vi hanno accesso.

Integrità

Le e i clienti possono fare affidamento sul fatto che i loro dati vengono modificati unicamente su esplicita richiesta. Per permettere alla clientela di modificare i propri criteri di recapito, la Posta mette a disposizione una procedura di login sicura sul sito web e nell'app.

Tracciabilità

Prima di giungere a destinazione un invio percorre un lungo cammino, durante il quale vengono registrate tutte le modifiche relative alla sua gestione. In questo modo la Posta si assicura che solamente le persone autorizzate possano apportare modifiche.

2020-072 (InfoSec) 06.2023

Accesso/identificazione

Le e i clienti possono verificare lo stato di un invio mediante un numero d'invio senza dover necessariamente effettuare l'accesso alla Post-App o al sito posta.ch. Se desiderano conoscere ulteriori dettagli sull'invio o registrare delle modifiche, devono accedere tramite nome utente e password personali. Questi dati di accesso per la Posta possono essere creati in tutta semplicità e sicurezza tramite SwissID. In casi particolari, come un cambiamento di indirizzo, la clientela riceve al proprio indirizzo e-mail registrato un codice di conferma, che costituisce un ulteriore elemento di sicurezza: la cosiddetta autenticazione a due fattori. In questo modo, la Posta scongiura qualsiasi tentativo di frode legato all'ordine di modifica.

In che modo può proteggersi la clientela?

I dati personali e le informazioni correlate devono essere tutelate con attenzione. Il semplice fatto di connettersi ai servizi sicuri della Posta, ad esempio tramite posta.ch o la Post-App, fornisce già una valida protezione di base. La clientela può aumentare il livello di sicurezza utilizzando password personali complesse. Per ottenere il massimo livello di protezione, queste ultime non dovrebbero essere condivise con nessuno. Se le e i clienti notano qualcosa di strano in relazione ai propri dati, la Posta li assiste in modo semplice e rapido su posta.ch, tramite app o presso la filiale più vicina.

2020-072 (InfoSec) 06.2023

Post-App

Le informazioni e prestazioni principali della Posta in un clic. Sempre e ovunque.

Descrizione del prodotto

Con la Post-App la clientela ha accesso alle prestazioni e alle informazioni principali della Posta 24 ore su 24 grazie a un login personale. L'app include i seguenti servizi: I miei invii (ad es. tracciamento degli invii, invito di ritiro, pick@home, Trattenere la corrispondenza), Ricerca ubicazioni, codice scanner e Web-StampVideo. L'elenco è ampliato di continuo in base alle esigenze della clientela.

Disponibilità

La Post-App è scaricabile dall'App Store di Google e Apple e utilizzabile sui dispositivi Android e iOS. Lato cliente, la disponibilità dell'app dipende dall'accesso a internet mobile o fisso ed eventualmente dalla performance del dispositivo mobile utilizzato. In generale, la disponibilità della Post-App e dei servizi che offre è elevata.

Riservatezza

La Post-App disponibile sugli App Store ufficiali presenta un elevato grado di riservatezza in quanto è stata sviluppata in proprio dalla Posta. I collegamenti e lo scambio di dati tra l'app e le prestazioni correlate sono codificati. I dati sensibili quali indirizzi della clientela e dati di invio non vengono memorizzati localmente nell'app. Per poter utilizzare le funzionalità protette della Post-App bisogna accedere con nome utente e password, il che costituisce un'ulteriore garanzia di sicurezza.

Integrità

La codifica dei collegamenti e dello scambio di dati tra l'app e i servizi collegati garantisce l'integrità dei dati. L'app verifica inoltre l'origine dei dati con un ulteriore meccanismo di sicurezza (certificato).

Tracciabilità

Le attività della Posta eseguite nei servizi collegati vengono registrate in modo tracciabile.

Accesso/identificazione

Per utilizzare le funzionalità protette della Post-App è necessario un account utente Posta con nome utente e password. I dati di login sono trasmessi in formato codificato. Le funzionalità avanzate della Post-App sono protette con il login SwissID.

2020-072 (InfoSec) 06.2023

Come può tutelarsi la clientela?

La clientela dovrebbe proteggere il dispositivo mobile utilizzato per mezzo di un PIN, del riconoscimento facciale o dell'impronta digitale, per evitare che in caso di smarrimento o furto del dispositivo terzi possano accedere facilmente alle sue informazioni (ad es. sulla Post-App).

La Post-App dovrebbe essere scaricata esclusivamente dagli App Store ufficiali di Android e Apple.

Si raccomanda di non rimuovere senza autorizzazione le limitazioni di utilizzo del dispositivo in uso (jailbreak), appositamente implementate dal produttore per motivi di sicurezza. Eliminando tali limitazioni possono verificarsi accessi non autorizzati al dispositivo, che possono portare, ad esempio, al furto di dati o all'accesso alle app bancarie.

2020-072 (InfoSec) 06.2023

Postshop

Shopping sicuro su Postshop. Numerose offerte in un solo clic.

Descrizione del prodotto

Postshop (postshop.ch) è lo shop online della Posta. Smartphone, articoli da ufficio e cartoleria e carte regalo: vi si possono trovare prodotti legati all'attività postale che semplificano la vita quotidiana della clientela. È anche possibile ordinare online e in tutta comodità gli ultimissimi francobolli della Posta e il materiale d'imballaggio per spedire lettere e pacchi. Al momento dell'acquisto la sicurezza è garantita dalla codifica delle informazioni e da una piattaforma di pagamento certificata.

Disponibilità

Postshop è disponibile 24 ore su 24, con rari periodi di interruzione. La Posta esegue periodicamente test di carico e verifica il rispetto del valore target prestabilito mediante un monitoraggio attivo.

Riservatezza

La Posta si assicura che i dati nello shop online possano essere consultati o pubblicati solamente dalle persone autorizzate a farlo. L'azienda analizza periodicamente il fabbisogno di protezione e il proprio piano di autorizzazione per l'accesso allo shop online, gestendo i dati in modo scrupoloso e attuando le disposizioni in materia di protezione dei dati e le prescrizioni di legge.

Integrità

La Posta verifica e ottimizza costantemente il proprio shop online. Prima di ogni aggiornamento di grande portata, incarica un organismo indipendente di effettuare test di sicurezza basati su standard internazionali (OWASP Top 10). Inoltre, Postshop fa parte del programma bug bounty della Posta, nel quadro del quale hacker etici vengono incaricati dalla Posta di identificare eventuali falle legate alla sicurezza, che vengono immediatamente corrette.

Tracciabilità

Un sistema di sorveglianza (monitoring) permette di escludere il rischio di modifica dei dati della clientela da parte di terzi su Postshop.

Accesso/identificazione

Chi desidera acquistare su Postshop può registrarsi tramite SwissID oppure ordinare come utente ospite. Gli acquisti contro fattura e la riscossione dei buoni sono invece possibili solo per la clientela il cui indirizzo è stato verificato tramite lettera. Alcuni articoli, come le carte regalo e i buoni elettronici, richiedono in ogni caso un pagamento immediato. Queste misure sono volte a ostacolare eventuali tentativi di frode.

2020-072 (InfoSec) 06.2023

In che modo può proteggersi la clientela?

Il modo migliore per proteggersi è gestire scrupolosamente sia la propria password SwissID sia i dati della propria carta PostFinance, della carta bancaria e della carta di credito. La password personale dovrebbe essere difficile da indovinare e utilizzata esclusivamente per SwissID. Per aumentare ulteriormente il livello di sicurezza, la clientela dovrebbe accedere direttamente nel portale della Posta, anziché tramite link in un'e-mail (inattesa) che potrebbe rappresentare un tentativo di phishing.

2020-072 (InfoSec) 06.2023

Sdoganamento di merci e invii

Importando ed esportando merci e invii con procedure sicure si garantiscono un'esecuzione e un recapito rapidi e, al tempo stesso, una gestione sicura dei dati degni di protezione.

Descrizione del prodotto

Quasi tutti gli operatori postali, compresa la Posta, sono associati all'Unione postale universale (UPU) e si attengono alle direttive dell'ente per ciò che concerne le condizioni di fornitura e le questioni relative alla fatturazione. Tra i consueti servizi postali rientrano gli incarichi di tipo doganale e fiscale, per i quali la Posta deve preparare e/o acquisire la documentazione rilevante ai fini della dichiarazione di sdoganamento. Il valore e, dunque, l'ammontare del tributo doganale è determinato sulla base dei dati dell'invio, con un processo sempre più evoluto e digitale.

Disponibilità

La clientela può registrare le informazioni relative all'invio (ad es. contenuto, peso e valore) che sono necessarie per la dichiarazione recandosi allo sportello o per via elettronica (ad es. tramite account utente su posta.ch o Post-App). Grazie alle opzioni digitali, la clientela non è più vincolata alle sedi e agli orari di apertura e può effettuare la registrazione in modo flessibile in qualsiasi momento e anche direttamente da casa.

Riservatezza

La Posta protegge i dati personali, i dati dell'invio e i contenuti della fattura da accessi non autorizzati. Elabora i dati della clientela e li mette anche a disposizione delle autorità doganali secondo gli obblighi imposti. Per il tracciamento degli invii e la fatturazione è indispensabile lo scambio sicuro di dati tra la clientela e la Posta, che viene garantito dal login cliente, da siti verificati e da collegamenti codificati con partner esterni.

Integrità

La clientela ha il diritto di esigere che i suoi dati possano essere modificati solo dalla Posta ed esclusivamente in casi motivati, ad esempio qualora debbano essere apportate modifiche al nome, all'indirizzo o ai dati del conto. Durante tutta la procedura di elaborazione i dati sono protetti e sicuri.

Tracciabilità

Il tragitto di un invio fino al suo destinatario è lungo, soprattutto in caso di importazione ed esportazione. A ogni passaggio dell'elaborazione l'invio viene scansionato. Assicurare la tracciabilità di un invio è fondamentale per la fase di sdoganamento al fine di poterlo trasportare correttamente e poter calcolare con esattezza i tributi doganali.

2020-072 (InfoSec) 06.2023

Accesso/identificazione

La Posta amplia di continuo i propri punti di contatto fisici e digitali, garantendo sempre l'identità della propria clientela per poterle comunicare contenuti importanti (ad es. l'invio) o farle pervenire informazioni sensibili a lei riservate attraverso il login cliente su posta.ch o dietro presentazione del rispettivo documento d'identità presso le filiali. L'identificazione è la chiave per accedere ai nostri servizi e ai dati ad essi correlati.

Come può tutelarsi la clientela?

Attraverso il phishing, i truffatori cercano di arrivare ai dettagli delle carte di credito di terzi, spesso richiedendo loro il pagamento di una fattura in sospeso. Ciò può succedere anche con i dati di un invio. Per questo la Posta invita a fare particolare attenzione. Quando non si ha impostato alcun invio presso la Posta o non si attende un ordine si dovrebbero ignorare queste e-mail di phishing. Qualora invece sia stato impostato o si attenda un invio, è meglio consultare la fattura nell'account utente della Posta o, in alternativa, rivolgersi alla filiale più vicina. In questo modo si ha la certezza dell'effettiva provenienza e regolarità della fattura.

Se si verificano situazioni insolite relative all'invio di lettere o pacchi, la nostra clientela può richiedere consulenza presso le filiali o chiamando il Contact Center. Se si ritiene di aver cliccato su un'e-mail troppo velocemente è opportuno cambiare subito la password o utilizzare l'autenticazione a due fattori.

2020-072 (InfoSec) 06.2023

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.

Descrizione del prodotto

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.

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.

2020-072 (InfoSec) 06.2023

2020-072 (InfoSec) 06.2023

Posta CH SA
Wankdorfallee 4
3030 Berna

N. tel. 0848 888 888
post@posta.ch
www.posta.ch