TrustTechnologies

Pomezia, 5 dicembre 2018

Oggetto: Integrazione delle Comunicazione relativa agli account del servizio di Posta Elettronica Certificata (PEC)

Gentile Utilizzatore,
desideriamo fornire di seguito alcune ulteriori informazioni relative all' attacco informatico che abbiamo subito ad opera di ignoti, nonché alcune informazioni presenti sul nostro servizio di PEC.

1. Descrizione sintetica dell'evento

Il 12 novembre 2018, si è verificata una violazione del servizio, che è stata da noi tempestivamente intercettata ed interrotta. L'attaccante è riuscito comunque nel suo intento di copiare alcuni dati identificativi dell'utenza contenuti nel database, ma non ha avuto accesso ai contenuti delle caselle del servizio e quindi delle comunicazioni testuali scambiate.
Scoperte le attività di violazione in corso, come misura di immediato contrasto, alle ore 17:30 circa del medesimo 12 novembre, abbiamo fermato il servizio e lo abbiamo ripristinato alle ore 20:00 circa, eliminando gli elementi che erano stati illecitamente utilizzati per perpetrare l'attacco. Da quel momento, la nostra attenzione si è concentrata sulle misure necessarie a prevenire la possibilità che l'attaccante sfruttasse eventuali dati acquisiti per accedere impropriamente alle caselle di PEC. Per questa ragione, abbiamo quindi disabilitato la possibilità di effettuare il reset della password utilizzando le domande con risposte segrete e riservando la possibilità di consegna dei codici di reset solo attraverso l'uso di SMS e email di posta ordinaria o tramite amministratori dei clienti o help desk di riferimento. Abbiamo conseguentemente effettuato interventi tesi a rendere inutilizzabili le password ed indispensabile il loro reset.
Le analisi e le attività di monitoraggio, condotte nel periodo successivo alla violazione, non hanno evidenziato comportamenti anomali nell'accesso alle caselle, né nelle operazioni di modifica o reset delle password.
Parallelamente, abbiamo ulteriormente rafforzato le misure di sicurezza già in uso a protezione del servizio.
In ogni caso, sono state prontamente interessate le Autorità, per ogni intervento di competenza.

2. Dati oggetto delle violazioni

Come indicato al punto precedente, il malintenzionato è riuscito ad appropriarsi indebitamente dei dati registrati nel servizio PEC. Questo è utilizzato da una Clientela molto diversificata, per la quale sono registrate le tipologie di dati di seguito indicate, in combinazioni diverse a scelta del cliente o dell'utente:

- username dell'utente per l'accesso ai servizi (in chiaro);
- dati di identità (in chiaro: nome, cognome, codice fiscale, data luogo e paese di nascita);
- dati del documento di identità (in chiaro: tipo, numero e scadenza);
- dati di residenza (in chiaro: indirizzo, comune, cap e provincia);
- dati di contatto telefonico (in chiaro: telefono, cellulare, fax);
- indirizzo email di posta ordinaria dell'utente (in chiaro);
- password di accesso (cifrate)

ad esempio, per alcuni clienti/utenti sono presenti solo nome e cognome, mentre per altri sono presenti anche quelli della data di nascita o del codice fiscale.
Inoltre, e solo nel caso di utilizzatori che avevano attivato la funzionalità di inoltro dei messaggi PEC verso posta elettronica ordinaria e configurato i relativi indirizzi, il malintenzionato ha fraudolentemente acquisito anche le informazioni seguenti:

- Indirizzo del destinatario e del mittente dei messaggi inoltrati;
- Indirizzo di posta elettronica ordinaria per l'inoltro dei propri messaggi PEC;
- Data e oggetto dei messaggi inoltrati.

3. Raccomandazioni per il singolo utilizzatore

In aggiunta alle azioni che abbiamo messo in campo, per massima prudenza e qualora non si fosse già provveduto, per proteggere i messaggi contenuti nelle caselle di PEC da accessi non autorizzati è comunque necessario che il singolo utilizzatore ponga in atto alcune operazioni essenziali, a lui solo riservate:

- Effettuare il reset della password utilizzando sms, casella di posta ordinaria o help desk, curando che essa abbia le necessarie caratteristiche di robustezza per la sua validità, come suggerite al momento del suo inserimento;
- Valutare la possibilità di attivare la modalità di reset della password, tramite SMS;
- Controllare in ogni caso lo stato dell'opzione di inoltro dei messaggi e disabilitarlo se necessario. Se si intende continuare ad utilizzarlo, verificare che le informazioni per l'inoltro siano corrette e se necessario modificarle;
- Accertarsi che sia sufficientemente robusta la password di accesso agli indirizzi di posta elettronica verso cui si attiva l'inoltro ed eventualmente cambiarla.

4. Rischi "potenziali" a seguito dell'acquisizione impropria dei dati personali

Indichiamo di seguito alcuni rischi "potenziali" cui possono essere esposti gli utilizzatori a seguito dell'acquisizione non autorizzata dei loro dati di tipologia confrontabile con quella oggetto della presente comunicazione:

- **Campagne di spam, phishing, malware e virus**: messe in atto sfruttando i recapiti telefonici o di posta elettronica che il malintenzionato potrebbe utilizzare per contattare il proprietario dei dati, fingendosi un altro soggetto (ad es. banche, aziende o ricercatori) ed ottenere ulteriori dati personali (anche di pagamento), o per inviare virus o software dannoso;
- **Furto di identità**: il malintenzionato potrebbe illecitamente proporsi, in sostituzione del legittimo titolare ed utilizzare tali dati per effettuare registrazioni a suo nome su siti e servizi online, oppure per tentare di stipulare contratti, etc.;
- **Altri comportamenti lesivi della privacy** messi in atto utilizzando i dati personali acquisiti, quali, ad esempio, l'osservazione di profili ed attività su social network.

Infine, sebbene le misure che abbiamo adottate rendano tale possibilità del tutto marginale, qualora il malintenzionato fosse riuscito ad utilizzare le credenziali per accedere alle caselle PEC, potrebbe utilizzarla per inviare comunicazioni false o acquisire il contenuto di documenti trasmessi tramite PEC. Ti chiediamo quindi di segnalare tempestivamente eventuali casi dubbi o comportamenti anomali agli amministratori o agli help desk di riferimento.

Puoi avere ulteriori informazioni sui dati personali trattati scrivendoci all'indirizzo: ti.tt@ttpec.telecomitalia.it .

Ci scusiamo per il disagio e, nel ricordare l'importanza di attuare le misure indicate al punto 3, inviamo cordiali saluti

TI Trust Technologies S.r.l.