Gentile Sig.ra/e

Le inviamo questa comunicazione perché i Suoi dati sono presenti all'interno degli archivi digitali di ISMEA, che sono stati oggetto di accesso abusivo da parte di soggetti non autorizzati che hanno eluso i nostri sistemi di protezione.

Dall'analisi condotta sull'incidente di sicurezza, riteniamo che le possibili conseguenze dell'accaduto possano essere le seguenti:

- i dati sottratti (compresi eventuali documenti di identità, nel caso siano stati forniti) potrebbero essere utilizzati per finalità diverse da quelle previste al momento della loro raccolta, oppure in modo non lecito: in particolare, per pubblicazione on line, per attività di riuso delle password (se fornite) acquisite illecitamente per violare altri sistemi (c.d. "*credential stuffing*"), di sottrazione fraudolenta di informazioni personali (c.d. "*phishing*"), di invio di pubblicità non richiesta (c.d. "*spamming*") e similari.

Stiamo facendo tutto quanto in nostro potere per risolvere il problema, limitando, per quanto possibile, i rischi.

Già nei momenti immediatamente successivi all'attacco abbiamo adottato le seguenti misure:

- l'infrastruttura digitale è stata posta in modalità off-line;
- è stata condotta un'analisi dettagliata del traffico del *firewall*;
- sono stati ripristinati tutti gli archivi e i servizi.

Abbiamo poi provveduto a fare denuncia alle Autorità competenti e all'Autorità Garante per la Privacy.

Continua il costante processo di aggiornamento e implementazione dei sistemi di sicurezza a protezione dell'infrastruttura digitale dell'Istituto. Pertanto, Le raccomandiamo di cambiare immediatamente le *password* utilizzate per l'accesso ai servizi di ISMEA.

Nel corso dell'esame analitico dei file interessati dall'accesso abusivo è appena emerso che tra i dati/documenti maggiormente delicati oggetto dell'attacco informatico è contenuto, per la categoria dei richiedenti di garanzie LTM, il documento di identità, il codice fiscale e la tessera sanitaria. Le consigliamo quindi di adottare le seguenti cautele:

- modificare le password di accesso eventualmente associate a servizi erogati in seguito ad identificazione mediante tessera sanitaria e documento di identità, e-mail comprese;
- monitorare eventuali messaggi anomali ricevuti via sms, pec, e-mail relativi a servizi non attivati da Lei o ad altre circostanze a Lei non note;
- verificare, se possibile con specifici motori di ricerca e/o servizi online, l'utilizzo anomalo del proprio Nome e Cognome nella Rete.

La informiamo infine che il Responsabile per la Protezione dei Dati (RPD, anche noto come DPO) di ISMEA è Gianluigi Ciacci, che potrà contattare, in caso di necessità, al seguente indirizzo pec: dpo@pec.ismea.it

Distinti saluti

ISMEA