Da: Laura Sala
A: [CG] Redazione Report
Oggetto: Richiesta intervista
Data: lunedì 9 novembre 2020 12:48:07

Gentile Redazione di Report,
inviamo le risposte, elaborate dagli uffici del Dipartimento per la trasformazione digitale, alle domande che ci avete post sull'app Immuni.

Cordiali saluti,
Laura Sala

È stata fatta una stima di quanti utenti effettivamente utilizzano l'app e quanti, invece, no, anche in base all'andamento dei contagi degli ultimi giorni?

La gestione dell'app "Immuni", in funzione dal primo giugno, non è affidata agli uffici della Ministra per l'Innovazione tecnologica e la Digitalizzazione che ne hanno curato una parte degli aspetti normativi e ne hanno curato e ne curano gli aspetti tecnologici. Il soggetto che ha la titolarità dei dati risulta dal decreto legge N.28 del 30 aprile 2020.

2. In base a uno studio dei ricercatori del Trinity College di Dublino è emerso che le app sviluppate sulla base delle Api di Google - tra cui anche Immuni - inviano dati personali anche sensibili ai server di Google sulla base del funzionamento del Google Play Services, un componente fondamentale per tutti i telefoni Android. Il Governo italiano era a conoscenza di questo dettaglio e ha mai avviato una interlocuzione con Google per cercare di arginare il problema?

Lo studio "*Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps*" scritto da due professori del Trinity College analizza, in particolare sotto il profilo privacy, alcuni sistemi di contact tracing europei distinguendo, fin dalle premesse, la componente "client" ovvero l'app progettata, sviluppata e gestita dalle autorità sanitarie nazionali dei diversi Paesi (Immuni nel nostro caso), e la componente del sistema Google sottostante.

Il giudizio degli autori sull'app Immuni – così come sulle app di Germania, Svizzera, Austria, Danimarca, Spagna, Polonia, Irlanda e Lettonia – è estremamente positivo: le app vengono espressamente considerate delle *best practice*.

Quanto al sistema Google sottostante, lo studio si limita a descrivere il processo di funzionamento caratteristico dell'intero ecosistema Google nell'ambito del quale, come è noto da sempre, vi è condivisione sistematica di informazioni tra il dispositivo dell'utente e la piattaforma attraverso la quale Google rende disponibili tutte le app, incluse, evidentemente, quelle destinate alla funzione di contact tracing.

Nulla nello studio, tuttavia, suggerisce che dati personali di carattere sanitario raccolti o gestiti attraverso le app di contact tracing nazionali, e in particolare Immuni, siano condivisi con Google o che Google vi abbia comunque accesso.

Tali dati vengono esclusivamente registrati sul dispositivo dell'utente e sono condivisi – in caso di accertamento di positività dell'utente – con i soli sistemi informatici del sistema sanitario nazionale. Così peraltro, nel caso di Immuni, è previsto dalla legge e accertato dal Garante per la Protezione dei dati personali in sede di parere sulla Valutazione di impatto relativa al funzionamento di Immuni predisposta dal Ministero della Salute.

3. Perché se la parte client-nazionale sviluppata da Bending Spoons è stata sottoposta a rigide limitazioni in base alla normativa europea e italiana, non sono stati fatti controlli o non si è imposto a un'azienda privata straniera come Google di rispettare la normativa privacy degli utenti italiani?

Immuni utilizza le API (Application Programming Interface) di contact tracing rese disponibili sui dispositivi con sistema operativo iOS e Android da Apple e Google. Tali soggetti non sono coinvolti nel trattamento dei dati personali degli utenti dell'app limitandosi ad assumere il ruolo di fornitori di tecnologia. Google e Apple, in ogni caso, sono tenuti a rispettare la disciplina in materia di protezione dei dati personali e sono soggetti al controllo del Garante per la Protezione dei dati personali.

4. Per quanto riguarda le possibili vulnerabilità delle app di contact tracing sviluppate sulle Api di Google e Apple e basate sulla tecnologia Bluetooth, sono state messe in campo mitigazioni del rischio derivanti da un possibile replay attack? Sono stati prodotti documenti che analizzano e valutano queste possibilità?

Come già spiegato a giornalisti che lo hanno chiesto, l'ipotetico attacco, chiamato nel gergo tecnico "relay", è possibile in via teorica come è stato riportato nella documentazione pubblica sull'applicazione, ma nella pratica è ritenuto particolarmente complicato da attuare. Necessiterebbe infatti dell'installazione sul territorio di numerose antenne fisiche ad alta potenza, facilmente individuabili. A renderlo ancora più complesso è poi il fatto che andrebbe condotto entro una finestra temporale ristretta e limitata. Se tale eventuale attacco dovesse mai avvenire, sarebbe rilevato dal sistema di notifiche e dalle segnalazioni degli utenti, consentendo un intervento locale.

https://github.com/immuni-app/immuni-documentation/issues/58