

UK ordina ad Apple di sbloccare iCloud, rischi per la sicurezza e la privacy



Il governo del **Regno Unito** ha recentemente emesso un ordine che impone ad Apple di fornire accesso ai **dati crittografati** degli utenti archiviati su **iCloud**, in caso di **inchieste rilevanti legalmente autorizzate**. Questa richiesta, avanzata ai sensi dell'**Investigatory Powers Act** del 2016, noto anche come "Snoopers' Charter", la carta dello spionaggio, solleva preoccupazioni significative riguardo alla **privacy** di tutti gli utenti Apple e alla sicurezza dei loro dati. Si tratta quindi di un precedente che potrebbe generare un pericoloso effetto domino.

Da parte di Apple e del Governo, vi è da notare che al momento però non è pervenuta nessuna replica. Vediamo allora insieme quali possono essere i possibili impatti e le conseguenze, qualora Apple decidesse di adeguarsi alla richiesta.

L'Investigatory Powers Act del 2016

L'Investigatory Powers Act è una legge britannica che conferisce alle autorità poteri estesi per raccogliere e accedere a dati elettronici. In particolare, consente al governo di emettere "**Technical Capability Notices**" (TCN), ordini legali, che obbligano le aziende tecnologiche a fornire mezzi per accedere ai dati degli utenti, anche se crittografati. Queste notifiche possono includere l'obbligo di creare **backdoor** nei sistemi di crittografia o di fornire chiavi di decrittazione. Con backdoor ci si riferisce invece, a un accesso nascosto o non documentato a un sistema informatico, a un software o a una rete, che permette di aggirare le normali procedure di sicurezza e autenticazione.

La richiesta del Governo britannico ad Apple

Secondo quanto riportato dal Washington Post, il governo britannico ha emesso proprio una TCN intimando ad Apple di creare una backdoor nel suo servizio iCloud, al fine di combattere il terrorismo e la criminalità internazionale. Questa richiesta non si limita agli utenti nel Regno Unito, ma si estende a livello globale, potenzialmente influenzando milioni di utenti Apple in tutto il mondo.

L'istanza del governo britannico ad Apple non è stata improvvisa, ma è il risultato di un processo iniziato anni prima. Già nel 2022, il governo del Regno Unito aveva espresso critiche nei confronti dei piani di Apple per introdurre una crittografia avanzata nel suo servizio cloud, sostenendo che questa misura avrebbe ostacolato le indagini su crimini particolarmente gravi. La situazione si è ulteriormente intensificata nei primi mesi del 2024, quando, secondo alcune indiscrezioni, l'Home Office avrebbe presentato ad Apple una bozza dell'ordine per l'introduzione di una backdoor.

Nel marzo 2024, durante un dibattito parlamentare sugli emendamenti all'Investigatory Powers Act, Apple ha formalmente avvertito il Parlamento britannico, sottolineando che l'adozione della legge avrebbe potuto costringere l'azienda a rimuovere importanti funzionalità di sicurezza per gli utenti nel Regno Unito. Infine, il mese scorso, il governo ha emesso ufficialmente l'ordine sotto forma di una "technical capability notice", rendendo esplicita la richiesta di accesso ai dati crittografati.

La richiesta del governo britannico non significa però che le autorità inizieranno improvvisamente a setacciare i dati degli utenti Apple. È logico pensare che l'accesso a iCloud sarà richiesto in presenza di un **grave rischio** per la sicurezza nazionale. In ogni caso, la richiesta delle autorità dovrebbe

essere **motivata** e seguire un procedimento giuridico, sulla base di indagini giudiziarie «autorizzate» e di «ragioni valide». Di contro Apple non può lamentarsene pubblicamente perché la legge britannica in oggetto, glielo impedisce.

La posizione di Apple sui dati iCloud

Apple ha storicamente resistito a richieste governative che potrebbero compromettere la sicurezza e la privacy dei suoi utenti. L'azienda offre una funzione chiamata "Protezione Avanzata dei Dati" per iCloud, che utilizza la crittografia end-to-end, garantendo che solo l'utente possa accedere ai propri dati. Nemmeno Apple ha accesso a queste informazioni.

Di fronte alla richiesta del governo britannico, Apple potrebbe considerare la possibilità di rimuovere la funzione "Protezione Avanzata dei Dati" per i backup iCloud solo nel Regno Unito invece di compromettere gli standard di sicurezza a cui ha abituato i suoi utenti. Questa opzione, tuttavia, non risolverebbe il problema, poiché il governo britannico chiede che l'accesso venga garantito anche per gli utenti al di fuori del territorio del Regno Unito. Si pensi al caso di un individuo indagato per attività sospette e residente in un altro Paese, ma con dati archiviati su iCloud.

Impatto e implicazioni globali

Se Apple dovesse conformarsi, potrebbe affrontare richieste simili da parte di governi di tutto il mondo, inclusi quelli con leggi sulla privacy meno rigorose. Questo solleva preoccupazioni significative riguardo alla privacy globale e alla sicurezza dei dati.

Alcuni esempi di paesi che potrebbero seguire l'esempio britannico:

- **Stati Uniti:** L'FBI ha più volte chiesto ad Apple e ad altre aziende tecnologiche di fornire accesso ai dati crittografati per indagini su terrorismo e criminalità organizzata. L'esempio britannico potrebbe fornire agli USA un nuovo argomento per chiedere lo stesso.
- **Unione Europea:** Anche se l'UE ha leggi sulla privacy più rigide (come il **GDPR**), alcuni stati membri potrebbero spingere per ottenere accesso ai dati crittografati in nome della sicurezza nazionale.
- **Cina:** Il governo cinese già impone restrizioni severe sulla tecnologia e la privacy. Se Apple concedesse l'accesso al Regno Unito, la Cina potrebbe chiedere lo stesso, aumentando la pressione sulle aziende tecnologiche per fornire strumenti di sorveglianza.
- **Russia e Medio Oriente:** Alcuni governi con scarsa trasparenza e rispetto dei diritti umani potrebbero usare questa situazione come scusa per ottenere un maggiore controllo sulle comunicazioni dei loro cittadini.

Ancora, se Apple fosse costretta a creare una backdoor per il Regno Unito, il rischio principale sarebbe che tale vulnerabilità venga **sfruttata anche da attori malevoli**, tra cui:

- **Hacker e cybercriminali:** Una backdoor nei sistemi di Apple potrebbe essere scoperta e utilizzata per accedere ai dati sensibili degli utenti, mettendo a rischio informazioni personali, finanziarie e aziendali.
- **Governi autoritari:** Alcuni stati potrebbero sfruttare il precedente per giustificare la vigilanza ed il controllo di massa e la repressione di oppositori politici.
- **Interferenze da parte di intelligence straniere:** Servizi segreti di paesi terzi potrebbero cercare di sfruttare le falle create per scopi di spionaggio e guerra informatica.

Una volta che una porta d'accesso viene creata, **non è più**

possibile garantire che venga usata solo dai governi “affidabili”.

Per quanto concerne invece le possibili conseguenze ed effetti sulle aziende tecnologiche e sul mercato globale, si evidenzia che le aziende concorrenti, come Google con Google Drive, Microsoft con OneDrive e Meta con WhatsApp e Messenger, potrebbero trovarsi sotto pressione per adottare misure simili, rischiando di compromettere la sicurezza dei loro utenti. Questo scenario potrebbe generare una perdita di fiducia nei servizi cloud, spingendo molte persone a cercare alternative che offrano una maggiore protezione della privacy.

Allo stesso tempo, le piattaforme che garantiscono una crittografia sicura senza backdoor, come ProtonMail, Signal e i servizi di cloud decentralizzato, potrebbero registrare un aumento significativo della loro base utenti. La vulnerabilità introdotta da una backdoor potrebbe inoltre indebolire la posizione competitiva delle aziende tecnologiche occidentali, favorendo la crescita di soluzioni alternative provenienti da mercati meno regolamentati, come quello cinese. Ciò potrebbe portare a una ridefinizione degli equilibri globali nel settore della sicurezza digitale e della protezione dei dati.

Reazioni e critiche

La richiesta del governo britannico ha suscitato critiche da parte di gruppi per la privacy e i diritti civili. Big Brother Watch, un'organizzazione per la privacy con sede nel Regno Unito, ha definito la mossa come una **“erosione storica”** della crittografia end-to-end.

Anche altre aziende tecnologiche, come Google e Meta, offrono servizi di archiviazione dati crittografati. Finora, dunque non è chiaro se abbiano ricevuto o meno richieste simili da parte del governo britannico.

Considerazioni legali ed etiche

L'istanza del governo britannico solleva quindi questioni legali ed etiche complesse. Da un lato, le autorità sostengono che l'accesso ai dati crittografati è essenziale per combattere il crimine e il terrorismo. Secondo questa prospettiva, fornire alle forze dell'ordine un accesso regolamentato ai dati degli utenti potrebbe migliorare l'efficacia delle operazioni contro il crimine organizzato, la pedopornografia e il terrorismo, evitando che le tecnologie crittografiche diventino uno strumento per nascondere attività illecite.

Dall'altro lato, gli esperti di privacy avvertono che, come sopra accennato, creare backdoor nei sistemi di crittografia potrebbe compromettere la sicurezza dei dati e violare i diritti alla privacy degli utenti. La crittografia non è solo uno strumento di protezione per criminali, ma anche un mezzo essenziale per difendere la privacy e la libertà di espressione di giornalisti, attivisti, dissidenti politici e cittadini comuni.

Questo crea quindi un **delicato equilibrio** tra le esigenze di sicurezza nazionale e la protezione dei diritti individuali.

A livello giuridico, la richiesta del governo britannico potrebbe entrare in conflitto con normative internazionali sulla protezione dei dati, come il **Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea**, che garantisce agli utenti il diritto alla riservatezza e impone alle aziende tecnologiche di adottare misure rigorose per proteggere le informazioni personali. Inoltre, l'introduzione di una backdoor potrebbe violare principi sanciti da trattati sui diritti umani, come l'**Articolo 12 della Dichiarazione Universale dei Diritti Umani**, che tutela la privacy e la protezione contro interferenze arbitrarie nella vita privata. Inoltre, la scelta di Apple potrebbe tradursi in una

pericolosa violazione dei diritti digitali a livello globale, trasformando la crittografia da strumento di protezione a potenziale meccanismo di sorveglianza.

Possibili scenari futuri

La situazione attuale evidenzia quindi le sfide in corso nel bilanciare la sicurezza nazionale con la privacy degli utenti. A seconda della risposta di Apple alla richiesta britannica, si possono delineare diversi scenari futuri, ognuno con implicazioni significative. Se Apple dovesse rifiutare di conformarsi, il governo britannico potrebbe reagire imponendo sanzioni o limitando l'accesso a determinati servizi Apple nel Regno Unito. L'azienda potrebbe rispondere lanciando una campagna pubblica a difesa della privacy, coinvolgendo altre imprese tecnologiche e organizzazioni per i diritti digitali. Questo scenario potrebbe anche sfociare in una lunga battaglia legale, con cause nei tribunali per stabilire la legittimità della richiesta governativa.

Se invece Apple accettasse di implementare una backdoor, la decisione potrebbe danneggiare la reputazione di Apple come azienda impegnata nella tutela della privacy, causando una perdita di fiducia da parte degli utenti e, di conseguenza, una diminuzione della clientela. Inoltre, governi meno democratici potrebbero sfruttare questa apertura per intensificare la sorveglianza sui propri cittadini, aggravando ulteriormente il problema della violazione dei diritti digitali.

Un'ulteriore possibilità è che Apple decida di modificare i suoi servizi solo per il Regno Unito, rimuovendo la crittografia end-to-end esclusivamente per gli utenti britannici, mentre nel resto del mondo i servizi rimarrebbero inalterati. Tuttavia, questa soluzione potrebbe rivelarsi **insufficiente**, dal momento che il governo britannico ha esplicitamente richiesto l'accesso anche ai dati di utenti non

residenti nel Regno Unito.

La strada intrapresa da Apple in risposta alla richiesta del governo britannico potrebbe avere implicazioni di vasta portata per il futuro della crittografia e della privacy digitale. Gli utenti e le aziende tecnologiche di tutto il mondo seguiranno da vicino gli sviluppi, consapevoli che le decisioni prese oggi potrebbero influenzare le politiche sulla privacy per gli anni a venire.

Conclusioni

La richiesta del governo britannico ad Apple di fornire accesso ai dati crittografati degli utenti riveste carattere **peculiare** e solleva questioni fondamentali sulla privacy di miliardi di utenti, la sicurezza e i diritti individuali. Mentre la tecnologia continua a evolversi, sarà infatti necessario trovare delle soluzioni per trovare un bilanciamento, in grado di proteggere sia la sicurezza nazionale che diritto fondamentale alla privacy dei cittadini.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/apple-dati-su-icloud/>