CLOUDFLARE

WHITEPAPER

Politiche di Cloudflare sulla privacy dei dati e le richieste delle autorità giudiziarie

Pubblicato il 28 gennaio 2021

Panoramica

La rete e l'attività di Cloudflare sono fondamentalmente tutte incentrate sulla fiducia dei clienti. Cerchiamo di guadagnare e mantenere continuamente quella fiducia progettando e distribuendo prodotti che migliorano la sicurezza dei nostri sistemi, crittografano i dati inattivi o in transito e consentono ai nostri clienti di determinare come viene ispezionato il traffico in diverse località in tutto il mondo.

Ma non tutte le sfide possono essere risolte grazie all'ingegneria. Per questo motivo, disponiamo anche di politiche e procedure che ci guidano nella gestione dei dati dei clienti e degli utenti finali sui nostri sistemi e che ci consentono di rispondere alle richieste di dati provenienti dal governo o da altre autorità giudiziarie.

Questo documento descrive queste politiche e fornisce i link a informazioni più dettagliate sui vari aspetti del nostro approccio alla privacy e alla conformità dei dati. In particolare, copre:

- **Il nostro punto di vista sul cambiamento del panorama della privacy dei dati**
- **Le nostre politiche relative alla privacy e alle richieste di dati**

Il panorama della privacy dei dati in continuo cambiamento

L'esplosione dei servizi cloud e il fatto che i dati possano essere archiviati al di fuori dei paesi di residenza di coloro che li hanno generati hanno rappresentato una sfida per i governi che conducono indagini giudiziarie. I provider di servizi online di ogni tipo, spesso, fungono da punto di accesso per questi registri elettronici.

Tuttavia, per i provider di servizi come Cloudflare, queste richieste possono rivelarsi spinose da gestire. Il lavoro svolto dalle forze dell'ordine e dalle altre autorità governative riveste grande importanza. Allo stesso tempo, i dati di cui le forze dell'ordine e le altre autorità governative sono alla ricerca non appartengono a noi. Utilizzando i nostri servizi, i nostri clienti ci hanno messo in una posizione di fiducia rispetto a quei dati. Mantenere questa fiducia è fondamentale per la nostra attività e per i nostri valori.

Queste tensioni sono esacerbate dal fatto che governi diversi hanno norme diverse per la protezione dei dati personali. Gli Stati Uniti, ad esempio, vietano alle aziende di divulgare il contenuto delle comunicazioni, anche ai governi non statunitensi, tranne che in determinate circostanze definite per legge. L'Unione europea (UE), che da tempo considera la privacy delle comunicazioni e la protezione dei dati personali come diritti umani fondamentali, protegge tutti i dati personali dell'UE tramite il Regolamento generale sulla protezione dei dati (GDPR). Sebbene queste protezioni si sovrappongano per certi aspetti, esse si differenziano sia nel loro ambito di applicazione che nei soggetti che tutelano.

Le differenze tra i quadri normativi sono importanti, in particolare quando si tratta di stabilire se le richieste legali di dati provenienti da governi esteri siano considerate conformi ai requisiti di privacy. Negli ultimi anni, ad esempio, la Corte di giustizia dell'Unione europea (CGUE) ha concluso in più occasioni che le restrizioni legali statunitensi in materia di raccolta dei dati, insieme ad alcuni impegni su base volontaria come il Privacy Shield (o il suo predecessore, il Safe Harbor USA-UE) non sono adeguati per il rispetto della normativa UE, in larga misura a causa delle leggi statunitensi che consentono alle autorità giudiziarie di raccogliere informazioni su cittadini non statunitensi a fini di intelligence. Di fatto, il Comitato europeo per la protezione dei dati (EDPB) ha assunto una posizione secondo cui una richiesta giudiziaria di dati da parte degli Stati Uniti, al di fuori di un procedimento legale in cui i Paesi dell'UE abbiano un certo controllo sulle informazioni prodotte, non rappresenta una base legittima per il trasferimento di dati personali soggetti al GDPR.

In fondo, si tratta di scontri per stabilire quando sia lecito che un governo possa utilizzare ordinanze o altri procedimenti giuridici per accedere ai dati di cittadini di un altro Paese. E questi scontri non stanno avvenendo solo in Europa. Nonostante le risposte delle rispettive politiche non siano omogenee, un numero crescente di paesi considera ora l'accesso ai dati dei propri cittadini una questione di sicurezza nazionale.

Le politiche di Cloudflare sulla privacy dei dati e le richieste di dati

Cloudflare ha da tempo implementato delle politiche che affrontano le problematiche in materia di accesso ai dati personali, sia perché crediamo sia la cosa giusta da fare, sia perché i conflitti giurisdizionali a cui oggi assistiamo sembravano inevitabili. Queste politiche riguardano:

- Impegno pubblico su come trattiamo i dati riservati e come gestiamo le richieste di tali dati da parte delle autorità giudiziarie
- Come informiamo i nostri clienti relativamente alle richieste di dati.

In generale, quando si verifica un conflitto tra due norme giuridiche differenti, noi scegliamo di default quella che tutela maggiormente la privacy. Ed esigiamo sempre che le richieste siano corredate dalle necessarie ingiunzioni legali. Ci comportiamo così perché, una volta "aperti i cancelli" per l'accesso ai dati, poi può essere estremamente difficile richiuderli.

Il nostro impegno pubblico in merito ai dati riservati e alle richieste delle autorità giudiziarie

A partire dal nostro primo rapporto sulla trasparenza in cui sono indicate in dettaglio le richieste di dati da parte delle autorità giudiziarie nel 2013, ci siamo impegnati pubblicamente su come affrontiamo le richieste di dati e abbiamo rilasciato dichiarazioni pubbliche sul modo in cui affrontiamo questioni per noi inedite. Queste ultime sono dette "warrant canary" con l'idea che rivestano una funzione di segnalazione al mondo esterno.

Queste "canary" hanno due funzioni. Per prima cosa sono una dichiarazione pubblica che non intraprenderemo queste azioni su base volontaria, nonché un meccanismo per trasmettere informazioni, tramite la rimozione della dichiarazione dal sito, che in caso contrario potrebbe esserci impedito di divulgare.

Le autorità di regolamentazione hanno iniziato a riconoscere il valore degli impegni in materia di privacy, in particolare quando possono essere fatti valere contrattualmente. Infatti, gli impegni che per anni abbiamo incluso nei nostri rapporti sulla trasparenza sono esattamente i tipi di impegni che la Commissione europea ha raccomandato di includere nella sua bozza di clausole contrattuali standard per la conformità al GDPR.

Ecco alcuni esempi dei nostri impegni alla data di pubblicazione di questo documento:

- **Non abbiamo mai installato alcun software o apparecchiatura delle forze dell'ordine nella nostra rete né abbiamo fornito feed di contenuti in transito nella nostra rete:** in qualità di società dedicata alla sicurezza, sappiamo che mantenere il controllo degli accessi alle nostre reti è un imperativo assoluto. Ecco perché il nostro team di sicurezza si è concentrato sul controllo, la registrazione e il monitoraggio degli accessi e viene sottoposto ogni anno a diverse valutazioni da parte di terzi. Vogliamo fare in modo che i nostri clienti capiscano che non vi è alcuna esenzione in tali controlli per le forze dell'ordine o altri soggetti governativi. Ecco perché affermiamo da un lato che Cloudflare non ha mai installato software o apparecchiature per le forze dell'ordine in nessun punto della nostra rete, e dall'altro che non abbiamo mai fornito ad alcuna organizzazione governativa un feed dei contenuti dei nostri clienti che transitano sulla nostra rete.
- **Non abbiamo mai condiviso la crittografia delle chiavi di autenticazione:** Cloudflare ritiene che una crittografia efficace, sia per i contenuti che per i metadati, sia necessaria per la privacy online. Se un Paese sta cercando di impedire a un servizio di intelligence esterno di accedere alle informazioni personali dei suoi cittadini, il primo passo dovrebbe essere la crittografia di tali informazioni personali. Ma i clienti e le autorità di regolamentazione devono anche essere sicuri che la stessa crittografia sia affidabile. Abbiamo quindi formalmente dichiarato di non aver mai consegnato ad alcuno le nostre chiavi di crittografia o di autenticazione, né quelle dei nostri clienti, e di non aver mai indebolito, compromesso o sovvertito la nostra crittografia su richiesta delle forze dell'ordine o di terzi.
- **Non abbiamo mai modificato i contenuti dei clienti né le richieste DNS:** non crediamo che i nostri sistemi debbano essere sfruttati per portare le persone su siti che non intendevano visitare o per modificare i contenuti che ottengono online. Pertanto, abbiamo dichiarato pubblicamente di non aver mai modificato i contenuti dei clienti né la destinazione prevista delle risposte DNS su richiesta delle forze dell'ordine o di terzi.
- **Trasparenza in merito a potenziali interruzioni dell'impegno:** ci siamo impegnati a contestare legalmente qualsiasi ordinanza che cerchi di farci interrompere questi impegni, in tribunale se necessario. Il nostro obiettivo era essere molto chiari, non solo nei confronti dei nostri clienti ma anche dei governi di tutto il mondo, su dove avremmo fissato i nostri limiti.

Sebbene la nostra filosofia generale sulla protezione dei dati sia rimasta invariata fin dalla nostra fondazione, occasionalmente adattiamo il nostro impegno in modo da riflettere gli ultimi cambiamenti nei nostri prodotti e nel panorama delle politiche. Un elenco definitivo aggiornato di tali impegni è disponibile nella nostra pagina del Rapporto sulla trasparenza.

Notificare ai nostri clienti richieste governative

Cloudflare ritiene da tempo che i nostri clienti meritino di essere informati quando qualcuno, comprese le forze dell'ordine o altri soggetti governativi, fa uso di un procedimento legale per richiedere i loro dati, in modo che possano contestarne la richiesta.

Infatti, fin dai nostri primi giorni come entità aziendale abbiamo adottato la politica di avvisare i nostri clienti in casi del genere. Nel gennaio 2013, quando avevamo meno di 30 dipendenti, l'FBI si presentò alla nostra porta con una lettera di sicurezza nazionale

che richiedeva informazioni su un cliente e e ci vietava di discuterne con chiunque tranne i nostri avvocati. All'epoca, le lettere di sicurezza nazionale (NSL, National Security Letter) non avevano quasi alcuna supervisione e potevano essere scritte e applicate da un unico ramo del governo degli Stati Uniti, imbavagliando i destinatari a tempo indeterminato.

Riconosciamo che potrebbero esserci alcune circostanze in cui potrebbe essere appropriato per le forze dell'ordine limitare temporaneamente la divulgazione per preservare la fattibilità di un'indagine. Tuttavia, riteniamo anche che il governo debba essere tenuto a giustificare qualsiasi disposizione di non divulgazione e che qualsiasi disposizione di non divulgazione debba essere esplicitamente limitata nel tempo minimo necessario per lo scopo in questione. Pertanto, abbiamo collaborato con la Electronic Frontier Foundation su una contestazione legale alla lettera. Il caso giudiziario che ne è derivato è durato diversi anni e siamo stati costretti a non parlarne fino al 2017. Ma alla fine, l'FBI ha ritirato la lettera.

Poiché i tribunali statunitensi hanno ipotizzato che le ordinanze di non divulgazione a tempo indeterminato sollevino problemi di costituzionalità, il Dipartimento di Giustizia degli Stati Uniti nel 2017 ha pubblicato delle linee guida incaricando i pubblici ministeri federali di limitare le ordinanze di non divulgazione a un periodo non superiore a un anno, salvo circostanze eccezionali. Ciò non ha tuttavia impedito a tutte le forze dell'ordine degli Stati Uniti di richiedere ordinanze di non divulgazione a tempo indefinito. Di fatto, dal 2017 abbiamo ricevuto almeno 28 ordinanze di non divulgazione senza una data di fine. In collaborazione con l'American Civil Liberties Union (ACLU), Cloudflare ha minacciato un'azione legale ogniqualvolta ha ricevuto tali ordinanze di non divulgazione a tempo indefinito. In ciascun caso, il governo ha successivamente inserito nelle ordinanze dei limiti temporali sugli obblighi di non divulgazione, consentendoci di dare comunicazione ai nostri clienti di tali richieste.

Affrontare i conflitti normativi

Mantenere il rispetto di normative come il GDPR, in particolare a fronte a ordinanze legali che potrebbero metterci nella difficile posizione di essere obbligati a violarlo, richiede il coinvolgimento dei tribunali. Un provider di servizi come Cloudflare può richiedere a un tribunale di annullare le ordinanze in ragione di un conflitto normativo, e ci siamo impegnati, sia nelle nostre dichiarazioni pubbliche che a livello contrattuale nel nostro Data Processing Addendum (DPA), a compiere questo passo, se necessario ad evitare tale conflitto. A nostro modo di vedere, il conflitto deve essere rimandato alla sua sede naturale: tra i due governi che battagliano su chi dovrebbe avere diritto ad accedere alle informazioni.

Conclusioni

Questo articolo è solo un'introduzione al nostro impegno esteso in materia di privacy dei dati.

Per maggiori informazioni su questo impegno, consulta:

- La nostra Informativa sulla privacy generale: descrive i dati che raccogliamo, come li utilizziamo, quali condividiamo e altre questioni comuni riguardanti la privacy.
- Il nostro rapporto sulla trasparenza: le informazioni aggiornate sulle richieste provenienti dalle autorità giudiziarie di divulgazione delle informazioni sui nostri clienti.
- La nostra pagina su privacy e compliance dei dati: gli ultimi annunci su come le nostre politiche e i nostri prodotti supportano le esigenze di privacy e compliance.

In definitiva, l'uso di una rete globale che protegga i clienti e i dati degli utenti finali e conforme alle leggi sulla privacy in tutto il mondo esige un ritorno a quei valori di cui ci siamo fatti promotori fin dalla prima ora: avere principi saldi ed essere trasparenti, rispettare la privacy, implementare procedure trasparenti e avvisare i clienti affinché possano prendere le proprie decisioni sui dati.

+44 20 3514 6970 | enterprise@cloudflare.com | cloudflare.com/it-it

REV:BDES-5987.2024JUL29