REPORT SUL PROTOCOLLO DI SICUREZZA NELL'UTILIZZO DI GOOGLE MEET

Estratto da "Guida di Amministratore di Google Workspace"

https://support.google.com/a/answer/7582940#privacy&zippy=%2Ccrittografia%2Cmisure-di-contrasto-ai-comportamenti-illeciti%2Csicurezza-del-deployment-dellaccesso-e-dei-controlli%2Crisposta-agli-incidenti%2Cbest-practice-per-la-sicurezza

Google è impegnata a creare prodotti che proteggano la privacy degli studenti e degli insegnanti e forniscano al tuo istituto la migliore sicurezza possibile.

- Dati dei clienti: le versioni Education, che includono Meet, non utilizzano i dati dei clienti a scopi pubblicitari. Google Cloud non vende i dati dei clienti a terze parti. Meet non include funzionalità o software che tracciano il livello di attenzione degli utenti.
- Trasparenza: Google si impegna a garantire la trasparenza delle norme e delle prassi relative alla raccolta dei dati. L'informativa sulla privacy della versione Education e il contratto illustrano i nostri obblighi contrattuali relativi alla protezione dei tuoi dati. Seguiamo una rigida procedura per rispondere alle richieste dei governi relative ai dati dei clienti e divulghiamo le informazioni sul numero e sul tipo di richieste che riceviamo dai governi tramite il Rapporto sulla trasparenza di Google.
- Controlli regolari: siamo sottoposti regolarmente a rigorosi controlli della sicurezza e della privacy per i nostri servizi cloud, incluso Meet.
- Conservazione dei dati: con Google Vault, gli amministratori possono impostare criteri di conservazione per le registrazioni di Meet archiviate su Google Drive. Questa funzionalità è utile per adempiere a obblighi legali.
- Funzionalità intelligenti e personalizzazione: gli utenti possono decidere se le funzionalità intelligenti in Gmail, Chat e Meet e le funzionalità di personalizzazione in altri prodotti Google possono utilizzare i dati di Gmail, Chat e Meet. Ulteriori informazioni relative a Funzionalità intelligenti e personalizzazione.

Google contribuisce a proteggere la tua privacy in diversi modi: consentendoti di mantenere il controllo, gestendo e sviluppando continuamente le funzionalità di sicurezza e rispettando le normative sulla protezione dei dati e altri standard di settore. In questo modo, puoi sfruttare i vantaggi di Meet:

- Controllo sui dati-Meet rispetta gli stessi impegni per la privacy e lo stesso livello di protezione dei dati degli altri servizi aziendali di Google Cloud. Ulteriori informazioni sulla privacy.
- I dati appartengono ai clienti, non a Google.
- Google non utilizza i dati dei clienti a fini pubblicitari e non li vende a terze parti.
- I dati dei clienti vengono criptati in transito e le registrazioni dei clienti archiviate su Google Drive vengono criptate a riposo per impostazione predefinita.
- Meet non dispone di funzionalità o software che tracciano il livello di attenzione degli utenti.
- Puoi configurare i criteri di conservazione per le registrazioni di Meet con Google Vault per adempiere alle obbligazioni legali.

Conformità: I nostri prodotti, incluso Meet, vengono regolarmente sottoposti a verifiche indipendenti dei controlli di sicurezza, privacy e conformità. Otteniamo costantemente certificazioni, attestazioni di conformità o rapporti di controllo in base agli standard globali. Per i casi in cui potrebbero non essere richiesti o applicati attestati o certificazioni formali abbiamo creato anche una serie di documenti di riferimento con risorse che permettono di rispettare la conformità a quadri e normative.

Ulteriori informazioni sulla conformità

Il nostro elenco globale di offerte relative alla conformità per Meet include:

- SOC 1/2/3
- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- Autorizzazione a operare (ATO) di livello moderato del FedRAMP
- Utilizzo conforme a HIPAA
- HITRUST CSF

- GDPR
- Quadro Privacy Shield (scudo per la privacy) (UE-USA e Svizzera-USA)
- BSI C5 (EMEA)
- ENS livello "High" (Spagna)
- MTCS livello 3 (Singapore)
- OSPAR (Singapore)
- CSA STAR

Trasparenza: Seguiamo una rigida procedura per rispondere a qualsiasi richiesta dei governi relativa ai dati dei clienti e divulghiamo le informazioni sul numero e sul tipo di richieste che riceviamo dai governi tramite il nostro Rapporto sulla trasparenza di Google.

Per contribuire a garantire la sicurezza e la privacy dei dati, Meet supporta le seguenti misure di **crittografia**:

- Per impostazione predefinita, per le riunioni video su browser web, nelle app Meet per Android e iOS e nelle sale riunioni con hardware Google Meet, tutti i dati di Meet vengono criptati durante il trasferimento tra il client e Google.
- Se partecipi a una riunione video via telefono, l'audio utilizza la rete dell'operatore telefonico e potrebbe non essere criptato.
- Le registrazioni di Meet archiviate su Google Drive vengono criptate a riposo per impostazione predefinita.
- Meet è conforme agli standard di sicurezza della IETF (Internet Engineering Task Force) per i protocolli DTLS (Datagram Transport Layer Security) e SRTP (Secure Real-Time Transport Protocol). Ulteriori informazioni su DTLS.

Per proteggere le riunioni video, Meet applica una vasta gamma di misure di **contrasto ai comportamenti illeciti**, tra cui controlli anti-compromissione sia per le riunioni video sul Web sia per le connessioni telefoniche. Di seguito sono riportate alcune delle principali misure di contrasto ai comportamenti illeciti adottate:

Browser web o app

- Codici riunione - Ogni codice riunione contiene 10 caratteri, estratti da un set di 25 caratteri. In questo modo diventa più difficile "indovinare" i codici riunione mediante attacchi di forza bruta.
- Dettagli della riunione - Possono essere modificati nell'invito. La modifica completa dell'invito alla riunione video comporta la modifica del codice riunione e del PIN del telefono. Questa operazione è particolarmente utile se un utente non fa più parte dell'invito alla riunione.
- Partecipare a una riunione - Quando le persone entrano in una riunione video, si applicano le seguenti limitazioni:
  - Gli utenti esterni possono entrare direttamente, ma solo se sono citati nell'invito di calendario o se sono stati invitati da partecipanti appartenenti al dominio dall'interno della sessione di Meet.
  - Qualsiasi altro utente esterno deve richiedere di partecipare alla riunione e la sua richiesta dovrà essere accettata da un membro dell'organizzazione ospitante.
  - Limitiamo la possibilità da parte di utenti esterni di partecipare alla riunione con un anticipo superiore a 15 minuti. Entro questo periodo di tempo, gli utenti esterni citati nell'invito di calendario possono entrare direttamente nella riunione.
  - Alcune funzionalità aggiuntive, come la possibilità per un utente che fa parte del dominio di rimuovere un invitato da una riunione, consentono ai partecipanti interni di avere un maggiore controllo sulla gestione dei comportamenti indesiderati durante le riunioni. Per ulteriori informazioni sugli invitati, consulta i record di controllo e usa lo strumento qualità Meet.

Telefonia

- PIN delle riunioni - I PIN sono generalmente composti da minimo nove cifre.
- Dettagli della riunione - Le combinazioni di numero di telefono e PIN non sono valide al di fuori dell'orario programmato per la riunione.
- Partecipare a una riunione - Le persone che partecipano via telefono non possono collegarsi alla riunione più di 15 minuti prima dell'orario programmato.

Se ritieni che qualcuno stia violando le Norme di utilizzo accettabile di Google Meet, puoi segnalare il comportamento illecito.

Meet offre diverse precauzioni per mantenere privati e protetti i tuoi dati:

- Accesso a Meet - Gli utenti dei browser Chrome, Mozilla Firefox, Apple Safari e Microsoft Edge non devono installare alcun plug-in o software. Meet funziona interamente nel browser. Questo limita l'esposizione di Meet agli attacchi e riduce la necessità di distribuire frequenti patch di sicurezza sui computer degli utenti finali. Sui dispositivi mobili, consigliamo di installare l'app Google Meet da Google Play (Android) o dall'App Store (iOS). Ulteriori informazioni su come accedere a Google Meet.
- Verifica in due passaggi - Supportiamo diverse opzioni per la verifica in due passaggi (V2P) per Meet: token di sicurezza, Google Authenticator, messaggio di Google e SMS.
- Programma di protezione avanzata - Gli utenti di Meet possono registrarsi al programma di protezione avanzata di Google. Questo programma, appositamente ideato per gli account ad alto rischio, offre le nostre protezioni più efficaci disponibili contro il phishing e i tentativi di compromissione degli account. Nessun membro del programma è stato oggetto di un tentativo riuscito di phishing, anche in caso di attacchi ripetuti.
- Altri metodi di autenticazione - L'accesso SSO (Single Sign-On) tramite SAML è disponibile per Meet in tutte le versioni di Google Workspace ed è possibile selezionare lo stack di autenticazione a più fattori (MFA) di Google quando si utilizza il provider di identità aziendale.
- Log - Il logging di controllo per Meet è disponibile nella Console di amministrazione. Ulteriori informazioni sul log di controllo di Google Meet
- Registrazioni - La funzionalità relativa alle aree geografiche dati può essere utilizzata per archiviare le registrazioni di Meet su Drive solo in determinate aree geografiche (ad esempio, Stati Uniti o Europa). Le limitazioni relative agli spazi di archiviazione specifiche per aree geografiche non si applicano a transcodifiche, elaborazione, indicizzazione ecc. dei video.

La gestione degli incidenti è un aspetto importante del programma generale di sicurezza e privacy di Google ed è fondamentale per rispettare le norme sulla privacy globali, come il GDPR. Abbiamo messo a punto procedure rigorose per la prevenzione, il rilevamento e la risposta agli incidenti.

Prevenzione degli incidenti

- Analisi automatizzata dei log di sistema e di rete - L'analisi automatizzata del traffico di rete e dell'accesso al sistema aiuta a identificare le attività sospette, illecite o non autorizzate, che vengono segnalate al personale addetto alla sicurezza di Google.
- Test - Il team addetto alla sicurezza di Google cerca attivamente potenziali minacce alla sicurezza utilizzando test di penetrazione, misure di controllo della qualità (QA), strumenti di rilevamento delle intrusioni e revisioni della sicurezza dei software.
- Revisioni del codice interno - La revisione del codice sorgente permette di rilevare vulnerabilità nascoste e problemi di progettazione, nonché verificare l'implementazione dei principali controlli di sicurezza.
- Programma a premi per il rilevamento delle vulnerabilità di Google - Le potenziali vulnerabilità tecniche nelle estensioni del browser di proprietà di Google e nelle applicazioni web e per dispositivi mobili, che potrebbero influire sulla riservatezza o sull'integrità dei dati utente, vengono talvolta segnalate da ricercatori di sicurezza esterni.

Rilevamento degli incidenti

- Strumenti e processi specifici del prodotto - Ove possibile, vengono utilizzati strumenti automatizzati per migliorare la capacità di Google di rilevare gli incidenti a livello di prodotto.
- Rilevamento delle anomalie di utilizzo - Google impiega diversi livelli di sistemi di machine learning per distinguere le attività utente sicure da quelle anomale riguardanti browser, dispositivi, accessi alle applicazioni e altri eventi di utilizzo.
- Avvisi di sicurezza dei servizi per data center e/o luoghi di lavoro - Gli avvisi di sicurezza nei data center eseguono un'analisi volta a rilevare incidenti che potrebbero influire sull'infrastruttura dell'azienda.

Risposta agli incidenti

- Incidenti di sicurezza - Google gestisce un programma di risposta agli incidenti di prim'ordine che offre queste funzioni chiave:
  - Sistemi di monitoraggio, analisi dei dati e servizi di machine learning pionieristici per rilevare e contenere preventivamente gli incidenti.
  - Esperti in materia che si dedicano esclusivamente agli incidenti relativi ai dati di qualsiasi tipo o dimensione.
  - Un processo maturo per avvisare tempestivamente i clienti interessati, in linea con gli impegni di Google indicati nei Termini di servizio e nei contratti con i clienti.

La creazione di uno spazio affidabile dedicato alle riunioni è importante per garantire un'esperienza sicura a tutti gli invitati.

- Fai attenzione quando condividi i link alle riunioni nei forum pubblici.
- Se lo screenshot di una riunione deve essere condiviso pubblicamente, assicurati che l'URL, situato nella barra degli indirizzi del browser, sia rimosso dallo screenshot.
- Prendi in considerazione l'utilizzo di Google Calendar per inviare inviti a riunioni private di Meet cui partecipa un gruppo fidato di partecipanti.
- Assicurati di controllare e accettare solo i nuovi invitati che riconosci prima di consentire loro di partecipare a una riunione.
- Se noti comportamenti indisciplinati durante una riunione, utilizza i controlli di sicurezza del moderatore, ad esempio per rimuovere un partecipante o disattivare il suo audio.
- Attiva la verifica in due passaggi per evitare che un altro utente assuma il controllo dell'account, anche nel caso si sia impossessato della tua password.
- Prendi in considerazione la registrazione al programma di protezione avanzata, il più efficace sistema di protezione di Google contro il phishing e la compromissione degli account.
- Esegui il Controllo sicurezza di Google. Abbiamo creato questo strumento passo passo per darti consigli per la sicurezza personalizzati e pratici finalizzati a rafforzare la sicurezza del tuo Account Google.