Sicurezza dei dispositivi mobili, delle app e dell'IoT

Proteggere dati e dispositivi in tutto il mondo

Noi di Google siamo impegnati più che mai a proteggere le persone, le organizzazioni e i governi condividendo le nostre competenze, mettendo la società nelle condizioni di affrontare i rischi informatici in continua evoluzione e lavorando continuamente per far progredire lo stato dell'arte della sicurezza informatica per costruire un mondo più sicuro per tutti.

Per questo motivo, è indispensabile per noi essere all'avanguardia e far evolvere costantemente le nostre soluzioni di sicurezza per affrontare il panorama in continua crescita delle minacce online, in particolare quando si tratta di proteggere tutti i dispositivi e le app connesse, al fine di fornire ai consumatori un ambiente sicuro in cui possano scegliere i dispositivi con cui interagire.

La sfida

La connettività ha un prezzo

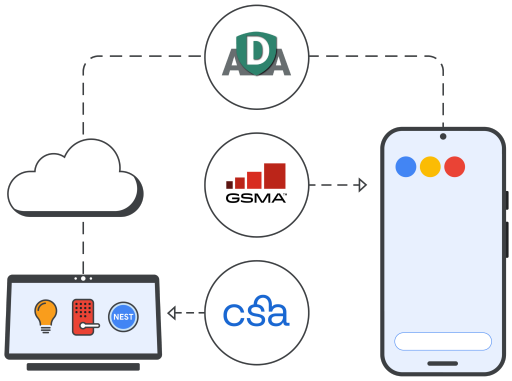
Gran parte della nostra vita quotidiana dipende dagli smartphone, dalle app e dai dispositivi connessi a Internet (IoT): passiamo sempre più tempo online condividendo sempre più dati preziosi, come informazioni bancarie o sanitarie. Per questo motivo, i criminali informatici più sofisticati stanno prendendo di mira questi dispositivi più che mai per ottenere informazioni sensibili.

Più dispositivi, più dati... più minacce

Si stima che oggi ci siano 17 miliardi di dispositivi IoT nel mondo, dalle stampanti ai sistemi di apertura dei garage, ognuno dei quali con software (alcuni open source) facilmente violabili.[1] Complessivamente, il numero di dispositivi IoT compromessi è quasi raddoppiato nel 2020.[2]

- Anche se siamo sempre più connessi attraverso i dispositivi IoT, non esistono standard globali per misurare la qualità della sicurezza dei prodotti connessi, così i consumatori si ritrovano a fare scelte non informate in fatto di sicurezza.
- I consumatori dovrebbero avere diritto alla trasparenza sui loro prodotti digitali, proprio come succede con gli ingredienti degli alimenti o dei prodotti per la pulizia che acquistano.
- I dispositivi mobili sono solo un vettore verso altre superfici di attacco e la capacità di interconnessione dei dispositivi aumenta la necessità di trasparenza in merito alla sicurezza su vasta scala. Pertanto, la sicurezza dell'ecosistema dei dispositivi connessi è importante quanto la sicurezza delle reti e dei sistemi.

La nostra collaborazione con organizzazioni del settore



La nostra soluzione

Noi di Google stiamo migliorando la sicurezza e la trasparenza dei nostri dispositivi connessi attraverso la sicurezza dei dispositivi mobili, delle app e dell'IoT:

Sicurezza dei dispositivi mobili

Android, il nostro sistema operativo open source, sfrutta un approccio multilivello alla sicurezza per i dispositivi mobili:

- Sicurezza multilivello
  - Avvio verificato, protezione anti roll-back e protezione dal ripristino di fabbrica garantiscono la versione di Android più recente e sicura.
  - L'autenticazione biometrica e con PIN protegge dagli accessi esterni.
  - "Trova il mio dispositivo" aiuta a localizzare il dispositivo e a ripristinarlo se viene smarrito o rubato.
- Protezione dell'identità e delle password
  - La verifica in due passaggi, il telefono come token di sicurezza e Gestore delle password proteggono il tuo account Google da accessi esterni.
  - Il Controllo sicurezza e il programma di protezione avanzata opzionale garantiscono un funzionamento sicuro e senza problemi del dispositivo.
- Protezione da phishing
  - "Telefono" di Google e "Messaggi" di Google aiutano a identificare e prevenire attacchi scam e phishing.
  - Google Navigazione sicura protegge oltre 5 miliardi di dispositivi in tutto il mondo.

Sicurezza delle app

L'anti-malware integrato aiuta a tenere alla larga le app dannose, mentre le informazioni sulla sicurezza dei dati garantiscono trasparenza agli utenti quando scaricano le app.

- Google Play Store: Gli strumenti di rilevamento basati sull'apprendimento automatico e gli analisti umani esaminano tutte le app prima che siano disponibili per il download. La sezione Sicurezza dei dati spiega quali tipi di dati vengono raccolti dall'app e per quali scopi vengono utilizzati.
- Google Play Protect: Analizza più di 125 miliardi di app ogni giorno e invia avvisi, le rimuove o le disattiva se vengono rilevati rischi per la sicurezza.
- App Defense Alliance (ADA): Google ha collaborato con i principali partner di rilevamento delle minacce su dispositivi mobili per lanciare l'App Defense Alliance, che aiuta a salvaguardare gli utenti Android dalle applicazioni potenzialmente dannose (PHA) attraverso informazioni condivise e un rilevamento coordinato.

Sicurezza dell'IoT

Le etichette di sicurezza dell'IoT indicano chiaramente le pratiche di privacy e sicurezza di un dispositivo, come ad esempio quali dati vengono raccolti.

- Crediamo in cinque principi chiave per gli schemi di etichettatura di sicurezza dell'IoT: etichette online (aggiornate in tempo reale), schemi di valutazione, linee guida sulla sicurezza abbinate a una certa flessibilità, ampia trasparenza e incentivi all'adozione.
- Collaboriamo con Connectivity Standards Alliance (CSA) e GSM Alliance (GSMA) per standardizzare un programma di certificazione a livello industriale per i requisiti normativi esistenti e futuri.

I nostri principi

Noi di Google applichiamo 3 principi chiave per migliorare la sicurezza e la trasparenza dei nostri dispositivi connessi:

Difesa in profondità: utilizziamo più livelli di architettura di sicurezza che insieme costruiscono una difesa solida in grado di funzionare in modo fluido ed efficace.

Apertura e trasparenza: la trasparenza è alla base della nostra filosofia. Informando gli utenti della nostra piattaforma e condividendo informazioni per rafforzare la nostra protezione, crediamo che un ecosistema open source possa essere più sicuro di uno chiuso.

Il meglio di Google e del nostro ecosistema: collaboriamo con team di esperti di Google e del settore per contribuire alla sicurezza di miliardi di utenti.

Applicazioni

Etichette di sicurezza dell'IoT: mettere il controllo nelle mani dei consumatori

Senza un'etichettatura di sicurezza dell'IoT definita, non esistono standard globali che i produttori di dispositivi possano seguire. Inoltre, gli utenti non hanno la trasparenza che meritano per sapere se i loro dispositivi proteggono i dati. Il settore deve trovare un terreno comune per far avanzare la sicurezza dell'IoT e restituire il controllo nelle mani dei consumatori. Stiamo lavorando a un sistema di etichettatura di sicurezza dell'IoT attraverso i nostri processi e le nostre partnership.

In primo luogo, investiamo in ricerche esterne sulla sicurezza per individuare le possibili vulnerabilità (Google Nest partecipa al vulnerability reward program di Google e offre ricompense ai ricercatori specializzati in sicurezza esterni a Google che trovano vulnerabilità).
Poi distribuiamo patch e correzioni di bug critici per almeno cinque anni dopo il lancio.
Tutti i nostri dispositivi sviluppati dal 2019 in poi utilizzano Avvio verificato per garantire l'esecuzione del software corretto e che l'accesso sia protetto. Ad esempio, i nostri dispositivi Google Nest vengono verificati tramite standard di sicurezza riconosciuti da terze parti, come quelli sviluppati da ETSI e ISO.

Questi standard, insieme al nostro ciclo di vita dello sviluppo del software (SDLC) riducono la probabilità che i consumatori siano esposti a pratiche di sicurezza inadeguate e aprono la strada a un'Internet aperta e più sicura.

I nostri investimenti e traguardi nel settore

2007 Creazione di Navigazione sicura per avvisare proattivamente gli utenti quando visitano siti web pericolosi: oggi protegge oltre 5 miliardi di dispositivi.

2010 Lancio del Rapporto sulla trasparenza di Google per mostrare come le politiche e le azioni di governi e aziende influenzano la privacy, la sicurezza e l'accesso alle informazioni online. Nel 2018 abbiamo aggiunto un Rapporto sulla trasparenza specifico per Android.

2017 Lancio di Google Play Protect che oggi è la soluzione anti-malware più diffusa e che analizza più di 125 miliardi di app al giorno su oltre 3 miliardi di dispositivi.

2019 Introdotti i token di sicurezza come funzione integrata su Android e poi su iPhone nel 2020.

2022 Google Play ha lanciato una sezione sulla Sicurezza dei dati per fornire maggiori informazioni su come le app raccolgono, condividono e proteggono i dati degli utenti, e ha avviato il primo sistema di badge per le app che hanno completato un controllo di sicurezza indipendente attraverso la App Defense Alliance.

2023 Passkey, per un futuro senza password viene messo in moto con un supporto esteso per le passkey dopo dieci anni trascorsi a promuovere gli standard aperti con la FIDO Alliance e i leader del tech di tutto il mondo.

Il nostro approccio

L'impegno per un mondo digitale aperto e sicuro

Con l'aumentare dei dati su un numero di dispositivi sempre maggiore su reti diverse, i problemi in merito alla sicurezza non potranno che crescere. Stiamo contribuendo a far progredire il futuro della sicurezza dei dispositivi connessi attraverso lo sviluppo di prodotti, i criteri di trasparenza e le partnership di settore.

Un caposaldo della nostra strategia di prodotto è la garanzia che i nostri prodotti siano secure by default. Navigazione sicura, Google Play Protect e i token di sicurezza integrati proteggono i dispositivi mobili e le app, fornendo il livello di sicurezza più alto nei nostri prodotti.

Contribuiamo a democratizzare le operazioni di sicurezza rendendo aperte e trasparenti le modalità di approccio ai problemi e condividendo le nostre conoscenze sulla sicurezza dei dispositivi connessi. Con il nostro approccio multilivello alla sicurezza, crediamo che un ecosistema open source possa essere più sicuro di uno chiuso.

Collaborando all'interno di CSA, ADA e GSMA, ci impegniamo per far progredire lo stato dell'arte della cybersicurezza per un'Internet e un futuro più sicuri per tutti.

Vogliamo alzare il livello di sicurezza dei dispositivi connessi e definire lo standard per un ambiente online più sicuro per tutti, ovunque. Scopri di più sui progressi di Google sulla sicurezza dei dispositivi connessi: g.co/connecteddevicesafety

Fonti: [1] CNBC Cyber Report, 9 gennaio 2023, 2 What is an IoT Attack? The Ins and Outs of IoT Security, 20 luglio 2021