Säkerhet på mobiler, appar och IoT

Skydda data och enheter över hela världen

Med den drastiska ökningen i antalet statsstödda cyberattacker och skadliga aktörer online anser vi att våra produkter och tjänster är mer användbara ju säkrare de är. Vi på Google fokuserar mer än någonsin på att skydda individer, organisationer och myndigheter genom att dela med oss av våra expertkunskaper, göra det möjligt för samhället att ta itu med ständigt föränderliga cyberrisker och hela tiden arbeta på att utveckla det senaste inom cybersäkerhet så att vi kan göra världen till en tryggare plats för alla.

Därför är det av största vikt att vi ligger steget före och hela tiden utvecklar våra säkerhetslösningar så att de klarar av den stadigt växande hotbilden, särskilt när det gäller att skydda alla uppkopplade enheter och appar. Vi vill tillhandahålla konsumenter en trygg miljö där de har inverkan på och möjlighet att välja vilka enheter de integrerar med.

Utmaning

Uppkoppling har ett pris

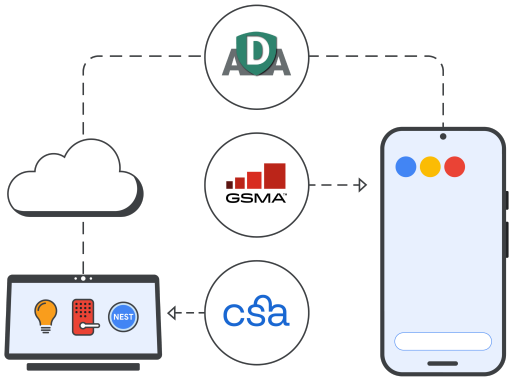
Smartphones, IoT-enheter och appar har blivit en stor del av vår vardag. Vi tillbringar mer och mer tid på nätet och delar mer och mer värdefulla data, som bank- eller hälsouppgifter. Avancerade nätbrottslingar riktar därför in sig mer på de här enheterna än tidigare, i hopp om att få tag på känslig information.

Fler enheter, mer data – och fler hot.

Det finns uppskattningsvis 17 miljarder IoT-enheter i världen just nu. Det är allt från skrivare till garageportöppnare, och alla innehåller massor av programvara (en del med öppen källkod) som enkelt kan hackas.[1] Det totala antalet IoT-enheter som har utsatts för intrång fördubblades nästan under 2020.[2]

- Vi blir allt mer ihopkopplade genom IoT-enheter, men det finns inga globala standarder för hur säkerhetskvaliteten för uppkopplade produkter ska mätas. Det leder till att konsumenter fattar beslut om enhetssäkerheten utan rätt information.
- Konsumenter ska ha möjlighet att få insyn om sina digitala produkter precis som de har rätt att få veta vilka ingredienser det finns i de livsmedel och rengöringsprodukter de köper.
- Mobila enheter är bara en vektor för andra attackytor, och förbindelsen mellan enheter ökar behovet för säkerhetsinsyn i stor skala. Säkerheten för ekosystemet av uppkopplade enheter är således lika viktig som nätverks- och systemsäkerhet.

Vårt samarbete med branschorganisationer



Vår lösning

På Google förbättrar vi säkerheten och insynen för våra uppkopplade enheter med hjälp av mobil-, app- och IoT-säkerhet:

Säkerhet på mobiler

Android, vårt operativsystem med öppen källkod, använder en säkerhetsmetod med flera lager för att skydda mobila enheter:

- Säkerhet i flera lager
  - Med verifierad uppstart, återställningsskydd och skydd mot fabriksåterställning får man den senaste och säkraste Android-versionen.
  - PIN-kod och biometrisk autentisering ser till att inga obehöriga får åtkomst.
  - Med Hitta min enhet kan man hitta eller rensa enheten om den har blivit stulen eller borttappad.
- Identitets- och lösenordsskydd
  - Tack vare Tvåstegsverifiering, Telefon som en säkerhetsnyckel och Lösenordshantering kommer obehöriga inte åt ditt Google-konto.
  - Säkerhetskontroll och Avancerat skydd, som är tillval, ser till att enheten fungerar smidigt och säkert.
- Skydd mot nätfiske
  - Phone by Google och Messages by Google gör det enklare att upptäcka och förhindra bedrägerier och nätfiskeattacker.
  - Google Säker webbsökning skyddar fler än fem miljarder enheter runtom i världen.

Appsäkerhet

Det finns ett skydd mot skadliga program som fungerar direkt och som håller skadliga appar borta. Datasäkerhetsinformation ger användarna insyn när de laddar ned appar.

- Google Play Butik: Identifieringsverktyg med maskininlärning och mänskliga analytiker granskar alla appar innan de kan laddas ned. I avsnittet om datasäkerhet står det vilka typer av data appar samlar in och vad dessa används till.
- Google Play Protect: Den här funktionen genomsöker mer än 125 miljarder appar varje dag och meddelar, tar bort eller inaktiverar om säkerhetsrisker upptäcks.
- App Defense Alliance (ADA): Google har samarbetat med de främsta partners inom hotidentifiering på mobiler för att lansera App Defense Alliance, som skyddar Android-användare mot potentiellt skadliga appar med hjälp av delad intelligens och samordnad identifiering.

IoT-säkerhet

IoT-säkerhetsetiketter visar tydligt integritets- och säkerhetspraxis för en enhet, till exempel vilka data som samlas in.

- Vi har fem grundprinciper för IoT-säkerhetsmärkning: liveetikett, utvärderingsscheman, säkerhetsriktlinjer tillsammans med flexibilitet, stor insyn och användningsincitament.
- Vi samarbetar med Connectivity Standards Alliance (CSA) och GSM Alliance (GSMA) för att standardisera ett certifikatprogram för hela branschen som uppfyller befintliga och kommande lagkrav.

Våra principer

På Google tillämpar vi tre grundprinciper för att förbättra säkerheten och insynen för våra uppkopplade enheter:

Djupgående försvar: Vi använder en arkitektur med flera lager av säkerhet som tillsammans utgör ett starkt försvar som fungerar smidigt och effektivt.

Öppet och transparent: Insyn är en viktig del av vår filosofi. Vi informerar våra plattformsansvändare och delar med oss av vår kunskap för att stärka vårt skydd. Vi tror nämligen att ett ekosystem med öppen källkod kan vara säkrare än ett stängt.

Det bästa från Google och vårt ekosystem: Vi samarbetar med olika expertteam på Google och i branschen för att skydda miljardtals användare.

Appar

IoT-säkerhetsetiketter ger konsumenter kontroll

Utan etablerad IoT-säkerhetsmärkning finns det inga globala standarder som enhetstillverkare kan följa. Användare får heller inte den insyn i hur data skyddas på enheterna som de förtjänar. Alla i branschen behöver samarbeta för att utveckla IoT-säkerheten och ge konsumenterna kontroll igen. Vi håller på att ta fram ett schema för IoT-säkerhetsmärkning med hjälp av våra processer och partnerskap.

Först och främst investerar vi i forskning om säkerhet på andra ställen än Google för att hitta möjliga säkerhetsrisker (Google Nest ingår i Googles belöningsprogram för den som identifierar säkerhetsrisker och ger belöningar till säkerhetsforskare utanför Google som hittar säkerhetsrisker).
Vi släpper sedan viktiga buggkorrigeringar och buggfixar i åtminstone fem år efter att något har lanserats.
På alla våra enheter som har tagits fram från och med 2019 används verifierad uppstart så att man kan vara säker på att det är rätt programvara som körs och att åtkomsten är skyddad. Våra Google Nest-enheter valideras till exempel med branschstandarder inom säkerhet från tredje part, bland annat de som har tagits fram av ETSI och ISO.

De här standarderna och vår säkra livscykel för programvaruutveckling (SDLC) minskar risken för att konsumenterna utsätts för dåliga säkerhetsrutiner och banar väg för ett mer öppet och säkrare internet.

Våra investeringar i branschen och milstolpar

2007 – Säker webbsökning etablerades så att användare proaktivt meddelas när de besöker farliga webbplatser och det skyddar nu fler än fem miljarder enheter.

2010 – Googles insynsrapport lanserades för att visa hur myndigheter och företagspolicyer och företagsåtgärder påverkar integritet, säkerhet och åtkomst till information online. 2018 lade vi till en särskild insynsrapport för Android.

2017 – Google Play Protect lanserades och den är nu en av de mest använda skyddslösningarna mot skadliga program och genomsöker fler än 125 miljarder appar varje dag på över tre miljarder enheter.

2019 – Säkerhetsnyckel infördes som en inbyggd funktion i Android och sedan för iPhone 2020.

2022 – Google Play lanserade ett avsnitt om datasäkerhet så att personer får mer information om hur appar samlar in, delar och skyddar användares data och startade det första märkessystemet för appar som har genomgått en fristående säkerhetsgranskning via App Defense Alliance.

2023 – Nyckel för en framtid utan lösenord körs igång med ett utökat stöd för säkerhetsnycklar efter ett årtionde där man har tagit fram öppna standarder med FIDO Alliance och ledande personer inom teknik världen över.

Vår metod

Vi strävar efter en öppen och säker digital värld

Säkerhetsproblem blir bara större med mer data på fler enheter i olika nätverk. Vi förbättrar den framtida säkerheten för uppkopplade enheter genom vår produktutveckling och våra insynsvillkor och branschpartnerskap.

En hörnsten i vår produktstrategi är att se till att våra produkter är säkra som standard. Säker webbsökning, Google Play Protect och inbyggda säkerhetsnycklar skyddar mobila enheter och appar så att våra produkter är så skyddade som möjligt.

Vi försöker att demokratisera säkerhetsåtgärder genom att vara öppna med och ge insyn i hur vi tar itu med problem och genom att dela med oss av vår kunskap om säkerhet för uppkopplade enheter. Vi anser att ett ekosystem med öppen källkod kan vara säkrare än ett stängt med vår mångalagrade säkerhetsmetod.

Vi strävar efter att utveckla det senaste inom cybersäkerhet för ett säkrare internet och en tryggare framtid för alla. Det gör vi genom att samarbeta med CSA, ADA och GSMA.

Vi jobbar hårt för att höja ribban för säkerhet för uppkopplade enheter och skapa en standard för en tryggare miljö online för alla överallt. Ta reda på mer om Googles framsteg när det gäller säkerhet för uppkopplade enheter: g.co/connecteddevicesafety

Källor: [1] CNBC:s cyberrapport, 9 jan. 2023, [2] What is an IoT Attack? The Ins and Outs of IoT Security, 20 juli 2021