Mobil-, app- og IoT-sikkerhed

Beskyttelse af data og enheder i hele verden

Med den dramatiske stigning i statsfinansierede cyberangreb og ondsindede onlineaktører, mener vi, at vores produkter og tjenester kun er så nyttige, som de er sikre. Hos Google er vi mere fokuserede end nogensinde på at beskytte mennesker, organisationer og regeringer ved at dele vores ekspertise, så vi kan gøre samfundet i stand til at håndtere cyberrisici, som hele tiden udvikles, og løbende arbejde for at forbedre det ypperste inden for cybersikkerhed for at skabe en sikrere verden for alle.

Som sådan er det bydende nødvendigt for os at være på forkant og konstant udvikle vores sikkerhedsløsninger for at tackle det stadigt voksende trusselslandskab, især når det kommer til at sikre alle forbundne enheder og apps, for at give forbrugerne et sikkert miljø, hvor de har handlekraft og valgmuligheder i de enheder, de anvender.

Udfordring

Forbindelse har sin pris

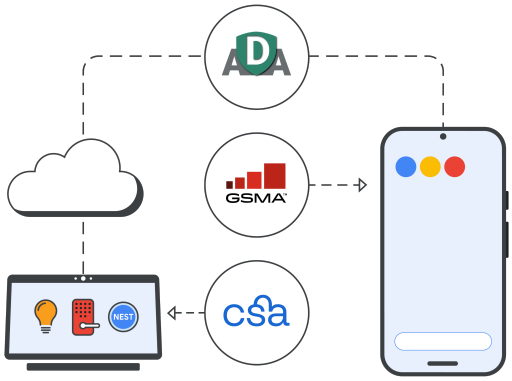
I dag er en stor del af vores liv forbundet med vores smartphones, apps og IoT-enheder – vi bruger mere og mere tid online og deler i processen flere og mere værdifulde data, som f.eks. bank- eller sundhedsoplysninger.

Flere enheder, mere data – flere trusler

Det anslås, at der nu er 17 milliarder IoT-enheder i verden, fra printere til garageportåbnere, hvor hver enkelt er pakket med software (nogle med open source), der nemt kan hackes.[1] Samlet set blev antallet af kompromitterede IoT-enheder næsten fordoblet i 2020.[2]

- Selvom vi er ved at blive tæt forbundet gennem IoT-enheder, er der ingen globale standarder for måling af sikkerhedskvaliteten af tilsluttede produkter, hvilket overlader det til forbrugerne at træffe uniformerede beslutninger om enhedernes sikkerhed.
- Forbrugere bør have ret til gennemsigtighed, når det gælder deres digitale produkter, ligesom de har ret til at vide, hvilke ingredienser der er i de fødevarer eller rengøringsartikler, de køber.
- Mobile enheder er kun én spreder til andre angrebsflader, og sammenkoblingen af enheder øger behovet for sikkerhedsgennemsigtighed i stor skala. Derfor er sikkerheden for forbundne enheders økosystem lige så vigtig som sikkerheden for netværk og systemer.

Vores samarbejde med brancheorganisationer



Vores løsning

Hos Google fremmer vi vores forbundne enheders sikkerhed og gennemsigtighed gennem mobil-, app- og IoT-sikkerhed:

Mobilsikkerhed

Android, vores open source-operativsystem, udnytter en lagdelt sikkerhedstilgang til at holde mobile enheder sikre:

- Lagdelt sikkerhed
  - Verified Boot, rollback-beskyttelse og fabriksnulstilling sikrer den nyeste og sikreste Android-version.
  - PIN-kode og biometrisk godkendelse beskytter mod adgang udefra.
  - 'Find min enhed' hjælper med at finde eller rydde enheden, hvis den bliver stjålet eller mistes.
- Beskyttelse af identitet og adgangskode
  - Totrinsbekræftelse, telefonen som sikkerhedsnøgle og adgangskodehåndtering beskytter din Google-konto mod adgang udefra.
  - Sikkerhedstjek og valgfri avanceret beskyttelse holder enheden kørende sikkert og problemfrit.
- Beskyttelse mod phishing
  - Phone by Google og Messages by Google hjælper med at opdage og forhindre svindel- og phishing-angreb.
  - Google Beskyttet browsing beskytter globalt over 5 milliarder enheder.

Appsikkerhed

Forudinstalleret anti-malware hjælper med at holde dårlige apps ude, og datasikkerhedsoplysninger giver brugerne gennemsigtighed, når de downloader apps.

- Google Play Butik: Maskinlærte sporingsværktøjer og menneskelige analytikere gennemgår alle apps, før de er tilgængelige til download. Afsnittet Datasikkerhed forklarer, hvilke typer data apps indsamler, og hvad disse data bruges til.
- Google Play Protect: Scanner mere end 125 milliarder apps hver dag og underretter, fjerner eller deaktiverer, hvis der opdages sikkerhedsrisici.
- App Defense Alliance (ADA): Google har samarbejdet med toppartnere inden for registrering af mobiltrusler for at lancere App Defense Alliance, der hjælper med at beskytte Android-brugere mod potentielt skadelige applikationer (PHA'er) gennem delt efterretning og koordineret sporing.

IoT-sikkerhed

IoT-sikkerhedsmærkninger kommunikerer tydeligt privatlivs- og sikkerhedspraksis på en enhed, f.eks. hvilke data der indsamles.

- Vi tror på fem kerneprincipper for IoT-sikkerhedsmærkningsordninger: live-label, evalueringsordninger, sikkerhedsgrundlag kombineret med fleksibilitet, omfattende gennemsigtighed og adoptionsincitamenter.
- Vi arbejder sammen med Connectivity Standards Alliance (CSA) og GSM Alliance (GSMA) for at standardisere et branchedækkende certificeringsprogram for eksisterende og fremtidige lovkrav.

Vores principper

Hos Google anvender vi tre kerneprincipper for at fremme vores forbundne enheders sikkerhed og gennemsigtighed:

Forsvar i dybden: Vi bruger flere lag af sikkerhedsarkitekturer, som arbejder sammen for at opbygge et stærkt forsvar, der kører problemfrit og effektivt.

Åbent og transparent: Gennemsigtighed er nøglen til vores filosofi. Ved at holde vores platformsbrugere informeret og dele viden for at styrke vores beskyttelse, mener vi, at et open source-økosystem kan være mere sikkert end et lukket.

Det bedste ved Google og vores økosystem: Vi samarbejder med ekspertteams på tværs af Google og branchen for at hjælpe med at holde milliarder af brugere sikre.

Applikationer

IoT-sikkerhedsmærkninger: Giver forbrugeren kontrollen

Uden etableret IoT-sikkerhedsmærkning er der ingen globale standarder, som enhedsproducenterne kan følge. Brugerne har heller ikke den indsigt, de fortjener, i om deres enheder beskytter deres data. Branchen må gå sammen for at drive IoT-sikkerheden fremad og give kontrollen tilbage til forbrugerne. Vi arbejder hen imod en IoT-sikkerhedsmærkningsordning gennem vores processer og partnerskaber.

Først investerer vi i ekstern sikkerhedsforskning for at lokalisere mulige sårbarheder (Google Nest deltager i Googles sårbarhedsbelønningsprogram og giver belønninger til sikkerhedsforskere uden for Google, der finder sårbarheder).

Derefter udsender vi vigtige korrektioner og fejlrettelser i mindst fem år efter lanceringen.

Alle vores enheder, der er udviklet i 2019 og senere, bruger Verified Boot for at sikre, at den rigtige software kører, og adgangen er beskyttet. For eksempel er vores Google Nest-enheder valideret ved hjælp af tredjeparts, brancheanerkendte sikkerhedsstandarder, som dem, der er udviklet af ETSI og ISO.

Disse standarder og vores sikre Software Development Life Cycle (SDLC) reducerer sandsynligheden for, at forbrugere vil blive udsat for dårlig sikkerhedspraksis, og baner vejen for et åbent, sikrere internet.

Vores brancheinvesteringer og milepæle

2007 Beskyttet browsing etableret for proaktivt at advare brugere, når de besøger farlige websteder, og det beskytter nu over 5 milliarder enheder.

2010 Google gennemsigtigheds-rapport lanceret for at vise, hvordan regeringer og virksomheders politikker og handlinger påvirker privatliv, sikkerhed og adgang til information online. I 2018 tilføjede vi en Android-specifik gennemsigtighedsrapport.

2017 Lancerede Google Play Protect, som nu er den mest udbredte anti-malware-løsning, der scanner over 125 milliarder apps om dagen på tværs af flere end tre milliarder enheder.

2019 Sikkerhedsnøgle blev introduceret som en indbygget funktion på Android og derefter til iPhone i 2020.

2022 Google Play lancerede en datasikkerhedssektion for at give folk flere oplysninger om, hvordan apps indsamler, deler og sikrer brugernes data, og startede det første badgesystem for alle apps, der har gennemført en uafhængig sikkerhedsgennemgang gennem App Defense Alliance.

2023 Passkey: fremtiden uden adgangskoder sættes i gang med udvidet adgangsnøgleunderstøtte lse efter et årti, hvor åbne standarder har været drevet med FIDO Alliance og teknologiledere verden over.

Vores tilgang

Dedikeret til en åben, sikker digital verden

Sikkerhedsbekymringer vil kun blive større med flere data på flere enheder på tværs af forskellige netværk. Vi hjælper med at styrke fremtiden for forbundne enheders sikkerhed gennem vores produktudvikling, gennemsigtighedskriterier og branchepartnerskaber

En hjørnesten i vores produktstrategi er at sikre, at vores produkter som standard er sikre. Beskyttet browsing, Google Play Protect og indbyggede sikkerhedsnøgler beskytter mobile enheder og apps for at give vores produkter det højeste niveau af sikkerhed.

Vi hjælper med at demokratisere sikkerhedsoperationer ved at være åbne og gennemsigtige i, hvordan vi tackler problemer, og ved at dele viden om sikkerhed i forbundne enheder. Vi mener, at et open source-økosystem med vores lagdelte sikkerhedstilgang kan være mere sikkert end et lukket.

Ved at samarbejde inden for CSA, ADA og GSMA stræber vi efter at fremme det nyeste inden for cybersikkerhed for et sikrere internet og en sikrere fremtid for alle.

Vi er dedikeret til at hæve barren for forbundne enheders sikkerhed og sætte standarden for et sikrere onlinemiljø for alle, overalt. Få flere oplysninger om Googles fremskridt inden for forbundne enheders sikkerhed: g.co/connecteddevicesafety

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