Zabezpečenie mobilných zariadení, aplikácií a IoT

Ochrana údajov a zariadení na celom svete

Veríme, že v súvislosti s dramatickým nárastom štátom sponzorovaných kybernetických útokov a škodlivých aktérov môžu byť naše služby užitočné, len ak sú bezpečné. V Googli sa viac než kedykoľvek predtým sústreďujeme na ochranu ľudí, organizácií a vlád tým, že zdieľame svoje odborné poznatky, umožňujeme spoločnosti riešiť neustále sa rozvíjajúce riziká a postupne pracujeme na pokroku v oblasti kybernetickej bezpečnosti s cieľom vybudovať bezpečnejší svet pre všetkých.

V prostredí, kde stále narastajú hrozby, je pre nás nesmierne dôležité, aby sme si udržali náskok a neustále vyvíjali naše riešenia bezpečnosti. Najmä pokiaľ ide o zabezpečenie všetkých pripojených zariadení a aplikácií s cieľom poskytnúť spotrebiteľom bezpečné prostredie, v ktorom sa budú môcť slobodne rozhodovať a budú mať kontrolu nad zariadeniami, s ktorými interagujú.

Výzva

Pripojenie má svoju cenu

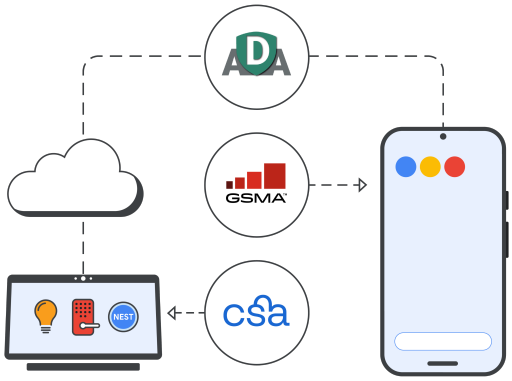
Veľkú časť svojich každodenných životov organizujeme pomocou smartfónov, aplikácií a zariadení IoT. Čím ďalej, tým viac času trávime online a zdieľame pritom čoraz viac cenných informácií, ako sú bankové alebo zdravotné údaje. Z tohto dôvodu sa prefíkaní páchatelia počítačovej kriminality častejšie zameriavajú na tieto zariadenia a snažia sa z nich získavať citlivé údaje.

Čím viac zariadení a údajov, tým väčšia hrozba

Odhaduje sa, že vo svete je momentálne 17 miliárd zariadení IoT, od tlačiarní až po zariadenia na otváranie garážových brán. Každé z nich má svoj softvér (niektoré sú open source), ktorý sa dá jednoducho napadnúť.[1] Celkovo sa počet napadnutých zariadení IoT v roku 2020 takmer zdvojnásobil.[2]

- Pomocou zariadení IoT sa všetko prepája, ale neexistujú žiadne globálne štandardy na meranie kvality bezpečnosti pripojených výrobkov. Spotrebitelia preto nemôžu prijímať informované rozhodnutia o ich zabezpečení.
- Spotrebitelia majú právo na transparentné informácie o svojich digitálnych výrobkoch rovnako, ako majú informácie o zložení potravín či čistiacich prostriedkov, ktoré si kupujú.
- Mobilné zariadenia pritom len otvárajú cestu k ďalším cieľom útokov a vzájomné prepojenie zariadení vo veľkej miere zvyšuje potrebu transparentnosti zabezpečenia. Preto je zabezpečenie ekosystému pripojených zariadení rovnako dôležité ako zabezpečenie sietí a systémov.

Naša spolupráca s odvetvovými organizáciami



Naše riešenie

V Googli zvyšujeme zabezpečenie a transparentnosť našich prepojených zariadení prostredníctvom zabezpečenia mobilných zariadení, aplikácií a IoT:

Zabezpečenie mobilných zariadení

Náš open source operačný systém Android chráni mobilné zariadenia pomocou viacstupňového zabezpečenia:

- Viacstupňové zabezpečenie
  - Overené spustenie, obnovenie pôvodných nastavení a ochrana po obnovení výrobných nastavení zabezpečujú, že je vždy nainštalovaná najnovšia a najbezpečnejšia verzia Androidu.
  - PIN a biometrické overenie chránia pred prístupom zvonku.
  - Funkcia Nájdi moje zariadenie určuje polohu zariadenia alebo z neho, v prípade krádeže či straty, vymaže údaje.
- Ochrana identity a hesiel
  - Dvojstupňové overenie, funkcia telefón ako bezpečnostný kľúč a Správca hesiel chránia váš účet Google pred prístupom zvonku.
  - Vďaka kontrole zabezpečenia a voliteľnej rozšírenej ochrane zariadenie funguje bezpečne a bez problémov.
- Ochrana pred phishingom
  - Telefón od Googlu a Správy od Googlu rozpoznávajú podvody a phishing a chránia pred nimi.
  - Bezpečné prehliadanie Googlu chráni viac než päť miliárd zariadení po celom svete.

Zabezpečenie aplikácií

Okamžitá ochrana proti malvéru chráni pred zlými aplikáciami a informácie o zabezpečení údajov zabezpečujú používateľom transparentnosť pri sťahovaní aplikácií.

- Obchod Google Play: pred tým než sú aplikácie k dispozícii na stiahnutie, ich skontrolujú detekčné nástroje so strojovým učením a analytici. Aké typy údajov aplikácie zbierajú a na čo sa používajú je vysvetlené v sekcii Zabezpečenie údajov.
- Google Play Protect: každý deň skontroluje viac než 125 miliárd aplikácií a ak zistí bezpečnostné hrozby, pošle upozornenie, odstráni ich alebo deaktivuje.
- App Defense Alliance (ADA): v spolupráci s poprednými partnermi v oblasti zisťovania hrozieb v mobilných zariadeniach Google spustil službu App Defense Alliance, ktorá pomocou zdieľania informácií a koordinovaného postupu pri odhaľovaní pomáha chrániť používateľov Androidu pred potenciálne škodlivými aplikáciami.

Zabezpečenie IoT

Štítky zabezpečenia IoT jasne určujú postupy ochrany osobných údajov v zariadení, ako napríklad ktoré údaje sa zbierajú.

- Pri postupe označovania zabezpečenia IoT sa riadime piatimi základnými princípmi: živé štítky, hodnotiace schémy, základy bezpečnosti spojené s flexibilitou, Hĺbková transparentnosť a motivácia na prijatie.
- Spolupracujeme s organizáciou Connectivity Standards Alliance (CSA) a GSM Alliance (GSMA) na štandardizácii certifikačného programu pre všetky existujúce a budúce regulačné požiadavky v rámci celého odvetvia.

Naše princípy

V Googli uplatňujeme tri základné princípy na zvýšenie zabezpečenia a transparentnosti našich prepojených zariadení:

Hĺbková ochrana: využívame viacúrovňovú bezpečnostnú architektúru, ktorá vo výsledku buduje silnú, hladkú a efektívnu ochranu.

Otvorenosť a transparentnosť: našou filozofiou je transparentnosť. Veríme, že informovaním používateľov našej platformy a zdieľaním poznatkov s cieľom posilniť zabezpečenie vytvoríme open source ekosystém, ktorý je bezpečnejší než uzavretý.

To najlepšie z Googlu a nášho ekosystému: spolupracujeme s tímami odborníkov v Googli a v odvetví, aby sme chránili miliardy používateľov.

Aplikácie

Štítky zabezpečenia IoT: kontrola v rukách spotrebiteľov

Okrem zavedených štítkov zabezpečenia IoT neexistujú iné globálne štandardy, ktorými by sa výrobcovia zariadení mohli riadiť. Používatelia takisto nemajú dostatočný prehľad o tom, či ich zariadenia chránia ich údaje. Aktéri v odvetví sa musia spojiť, aby vyvinuli tlak na zlepšenie zabezpečenia IoT a vrátili kontrolu do rúk spotrebiteľov. V rámci rôznych procesov a partnerstiev pracujeme na vytvorení postupu označovania zabezpečenia IoT.

Najprv investujeme do externého výskumu v oblasti bezpečnosti, aby sme určili možné nedostatky v zabezpečení (Google Nest je súčasťou programu odmien za nahlásenie chýb zabezpečenia Googlu a odmeňuje výskumníkov v oblasti zabezpečenia mimo Googlu, ktorí odhalia nedostatky v zabezpečení).
Následne najneskôr do piatich rokov po spustení riešime kritické chyby.
Všetky naše zariadenia vytvorené v roku 2019 alebo neskôr prejdú overeným spustením, čo zaručí, že používajú správnu verziu softvéru a prístup je chránený. Napríklad zariadenia Google Nest sa overujú na základe bezpečnostných štandardov tretích strán, ktoré sú uznávané v odvetví, ako napríklad štandardy určené normami ETSI a ISO.

Tieto štandardy a náš bezpečný životný cyklus vývoja softvérov znižujú pravdepodobnosť, že budú spotrebitelia čeliť nedostatočnej bezpečnosti, a predstavujú cestu k otvorenému a bezpečnejšiemu internetu.

Naše investície do odvetvia a míľniky

2007 – **Zavedenie bezpečného prehliadania**, ktoré používateľov proaktívne upozorňuje, keď navštívia nebezpečné weby, a momentálne chráni už viac ako päť miliárd zariadení.

2010 – **Zavedenie Informácií o transparentnosti od Googlu**, ktoré ukazujú, ako vládne a firemné pravidlá a kroky ovplyvňujú súkromie, zabezpečenie a prístup k informáciám online. V roku 2018 sme doplnili Informácie o transparentnosti pre Androidy.

2017 – **Spustenie služby Google Play Protect**, ktorá je teraz najpoužívanejším riešením proti malvéru a skenuje vyše 125 miliárd aplikácií na viac než troch miliardách zariadení.

2019 – **Zavedenie bezpečnostného kľúča** ako zabudovanej funkcie v zariadeniach s Androidom a v roku 2020 aj v zariadeniach iPhone.

2022 – **V službe Google Play** bola spustená sekcia Zabezpečenie údajov, v ktorej používatelia nájdu viac informácií o tom, ako aplikácie zbierajú, zdieľajú a chránia ich údaje. Zároveň bol spustený prvý systém odznakov pre aplikácie, ktoré prešli nezávislou kontrolou zabezpečenia v App Defense Alliance.

2023 – **Prístupový kľúč: budúcnosť bez hesiel** sa spúšťa s rozšírenou podporou po desaťročí presadzovania otvorených štandardov s alianciou FIDO a technologickými lídrami na celom svete.

Náš prístup

Sme zaviazaní budovať otvorený a bezpečný digitálny svet

S pribúdajúcim množstvom údajov a zariadení na rôznych sieťach sa obavy o bezpečnosť takisto len zvyšujú. Pomáhame napredovať v oblasti zabezpečenia pripojených zariadení prostredníctvom vývoja našich produktov, kritérií transparentnosti a partnerstiev v rámci odvetvia

Základným kameňom našej produktovej stratégie je zabezpečiť, aby naše produkty spĺňali štandardy zabezpečenia. Bezpečné prehliadanie, Google Play Protect a vstavané bezpečnostné kľúče chránia mobilné zariadenia a aplikácie a poskytujú našim produktom najvyššiu úroveň zabezpečenia.

Pomáhame demokratizovať bezpečnostné operácie tým, že sme otvorení a transparentní v riešení problémov a zdieľame poznatky o zabezpečení pripojených zariadení. Veríme, že pomocou viacstupňového zabezpečenia vytvoríme open source ekosystém, ktorý je bezpečnejší než uzavretý.

Spoluprácou s organizáciami CSA, ADA a GSMA sa snažíme zlepšiť momentálny stav kybernetickej bezpečnosti a vytvárať bezpečnejší internet a budúcnosť pre všetkých.

Zaviazali sme sa zvýšiť úroveň zabezpečenia pripojených zariadení a nastaviť štandard pre bezpečnejšie online prostredie pre všetkých a kdekoľvek. Ďalšie informácie o pokroku Googlu v oblasti zabezpečenia pripojených zariadení: g.co/connecteddevicesafety

Zdroje: [1] CNBC Cyber Report (Správa o kybernetickej bezpečnosti organizácie CNBC), 9. januára 2023, [2] What is an IoT Attack? The Ins and Outs of IoT Security (Čo je IoT útok? Plusy a mínusy zabezpečenia IoT), 20. júla 2021