Securitatea dispozitivelor mobile, a aplicațiilor și a IoT

Protejăm datele și dispozitivele din întreaga lume

Dată fiind creșterea puternică a atacurilor cibernetice sponsorizate de anumite state și a actorilor rău-intenționați online, credem că produsele și serviciile noastre sunt utile doar în măsura în care sunt securizate. La Google, suntem mai concentrați ca niciodată să protejăm oamenii, organizațiile și autoritățile guvernamentale prin împărtășirea experienței noastre, să ajutăm societatea să facă față riscurilor cibernetice din ce în ce mai mari și să lucrăm permanent pentru a dezvolta o securitate cibernetică de vârf, în vederea construirii unei lumi mai sigure pentru toți oamenii.

Prin urmare, este imperativ pentru noi să fim cu un pas înaintea evoluțiilor și să ne dezvoltăm permanent soluțiile de securitate pentru a face față peisajului în continuă schimbare al amenințărilor, în special în ceea ce privește securizarea tuturor dispozitivelor și aplicațiilor conectate, pentru a le oferi clienților un mediu sigur, în care să aibă posibilitatea și opțiunea de a alege dispozitivele cu care intră în legătură.

Provocarea

Conectivitatea implică un preț

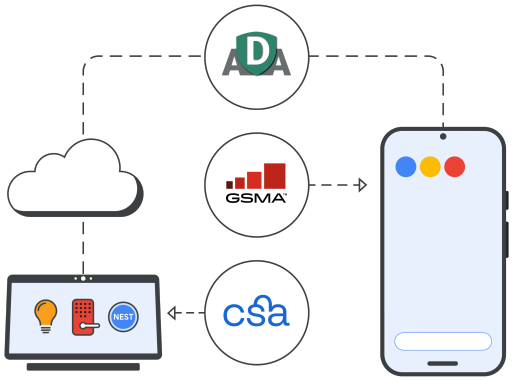
Ne desfășurăm o parte atât de importantă din viețile noastre zilnice cu ajutorul smartphone-urilor, aplicațiilor și dispozitivelor IoT—petrecând din ce în ce mai mult timp și partajând din ce în ce mai multe date valoroase, cum ar fi informațiile bancare și medicale, în acest proces. Din această cauză, infractorii cibernetici sofisticați vizează aceste dispozitive mai mult ca niciodată până acum, pentru a obține informații sensibile.

Mai multe dispozitive, mai multe date–mai multe amenințări

Se estimează că în acest moment există 17 miliarde de dispozitive IoT în lume, de la imprimante la dispozitive de deschidere a garajelor, fiecare echipat cu software (unele din surse deschise) care poate fi atacat ușor.[1] Per total, numărul de dispozitive IoT compromise aproape s-a dublat în 2020.[2]

- Cu toate că devenim profund conectați prin dispozitive IoT, nu există standarde globale pentru măsurarea calității securității produselor conectate, ceea ce îi face pe utilizatori să ia decizii neinformate în ceea ce privește securitatea dispozitivelor.
- Utilizatorii ar trebui să aibă dreptul la transparență în legătură cu produsele lor digitale, așa cum au dreptul să cunoască ce ingrediente sunt în alimentele pe care le consumă sau în produsele de curățenie pe care le cumpără.
- Dispozitivele mobile sunt doar un vector spre alte suprafețe de atac și interconectivitatea dispozitivelor crește nevoia de transparență a securității pe scară largă. De aceea, securitatea ecosistemului de dispozitive conectate este la fel de importantă ca securitatea rețelelor și a sistemelor.

Colaborarea noastră cu organizațiile din industrie



Soluția noastră

La Google, dezvoltăm securitatea și transparența dispozitivelor noastre conectate, prin securitatea dispozitivelor mobile, a aplicațiilor și a IoT:

Securitatea dispozitivelor mobile

Android, sistemul nostru de operare din surse deschise, utilizează o abordare a securității în straturi, pentru a menține dispozitivele mobile în siguranță:

- Securitate pe mai multe niveluri
  - Inițializarea verificată, protecția retroactivă și protecția resetării la setările din fabrică asigură cea mai recentă și mai sigură versiune Android.
  - Autentificarea prin cod PIN și date biometrice protejează împotriva accesului din exterior.
  - „Găsește-mi dispozitivul” ajută la localizarea dispozitivului sau la ștergerea acestuia în caz de furt sau pierdere.
- Protecția identității și a parolei
  - Verificarea în 2 pași, telefonul ca o cheie de securitate și managerul de parole protejează contul Google împotriva accesului din exterior.
  - Verificarea securității și protecția avansată opțională mențin funcționarea dispozitivului în siguranță și în parametri.
- Protecția anti-phishing
  - Telefon de la Google și Mesaje de la Google ajută la detectarea și prevenirea atacurilor de scam și phishing.
  - Navigarea sigură Google protejează peste 5 miliarde de dispozitive la nivel global.

Securitatea aplicațiilor

Aplicațiile anti-malware incluse încă de la livrare sunt utile pentru menținerea distanței față de aplicațiile rău-intenționate, iar informațiile despre securitatea datelor oferă transparență utilizatorilor atunci când descarcă aplicațiile.

- Google Play Store: Instrumentele de detecție cu învățare automată și analiștii umani verifică toate aplicațiile înainte de a le pune la dispoziție pentru descărcare. Secțiunea de securitate a datelor explică ce tipuri de date colectează aplicațiile și pentru ce sunt utilizate datele.
- Google Play Protect: Scanează peste 125 de miliarde de aplicații în fiecare zi și notifică, elimină sau dezactivează, dacă sunt detectate riscuri de securitate.
- App Defense Alliance (ADA): Google a colaborat cu parteneri de top în domeniul detectării amenințărilor mobile pentru a lansa App Defense Alliance (Alianța pentru Protecția Aplicațiilor), care ajută la protecția utilizatorilor împotriva Aplicațiilor Potențial Periculoase (PHA), prin informații partajate și detectare coordonată.

Securitatea IoT

Etichetele de securitate IoT transmit practici de confidențialitate și securitate pe un dispozitiv, cum ar fi tipul de date colectate.

- Credem în cinci principii esențiale pentru schemele de etichetare IoT: eticheta live, schemele de evaluare, nivelurile de securitate de bază cuplate cu flexibilitate, transparență și stimulente de adoptare.
- Lucrăm cu Connectivity Standards Alliance - Alianța Standardelor de Conectivitate (CSA) și GSM Alliance - Alianța GSM (GSMA) pentru a standardiza un program de certificare la nivel de industrie, pentru cerințele de reglementare actuale și viitoare.

Principiile noastre

La Google, aplicăm 3 principii esențiale pentru dezvoltarea securității și transparenței dispozitivelor noastre conectate:

Protecția în profunzime: Utilizăm mai multe straturi ale arhitecturii de securitate, care funcționează împreună pentru a asigura o protecție puternică și eficientă, în parametri optimi.

Deschidere și transparență: Transparența este cheia filosofiei noastre. Ținându-i la curent pe utilizatorii platformelor noastre și oferindu-le cunoștințele pentru a ne consolida protecția, credem că un ecosistem din surse deschise poate fi mai sigur decât unul închis.

Cea mai bună variantă a Google și a ecosistemului nostru: Colaborăm cu echipe de experți din cadrul Google și din industrie pentru a ajuta la păstrarea siguranței pentru miliarde de utilizatori.

Aplicații

Etichetele de securitate IoT: transferul controlului în mâinile utilizatorilor

Fără o etichetare de securitate IoT clară, nu există standarde globale pe care producătorii de dispozitive să le respecte. Nici utilizatorii nu au vizibilitatea pe care o merită, pentru a ști dacă dispozitivele lor le protejează datele. Companiile din industrie trebuie să își unească forțele pentru a împinge securitatea IoT înainte și pentru a readuce controlul în mâinile utilizatorilor. Depunem eforturi pentru a crea o schemă de etichetare a securității IoT prin procesele și parteneriatele noastre.

În primul rând, investim în cercetarea securității din exterior pentru a identifica posibilele vulnerabilități (Google Nest participă la programul Google de recompense pentru descoperirea vulnerabilităților și oferă recompense pentru cercetătorii din domeniul securității din afara Google, care găsesc vulnerabilități).

Ulterior, lansăm patchuri și remedieri ale erorilor critice pentru cel puțin cinci ani după lansare.

Toate dispozitivele noastre dezvoltate în 2019 și ulterior utilizează Inițializarea verificată pentru a asigura rularea software-ului potrivit și protecția accesului. De exemplu, dispozitivele noastre Google Nest sunt validate folosind standarde terțe, recunoscute în industrie, cum ar fi cele dezvoltate de ETSI și ISO.

Aceste standarde și Software Development Life Cycle - Ciclul de viață al dezvoltării software (SDLC) securizat reduc posibilitatea ca utilizatorii să fie expuși la practici de securitate necorespunzătoare și deschid drumul spre un internet deschis, mai sigur.

Investițiile noastre în industrie și momentele semnificative

2007 – **Navigarea sigură a fost introdusă** pentru a alerta în mod proactiv utilizatorii când vizitează site-uri web periculoase și protejează, acum, peste 5 miliarde de dispozitive.

2010 – **Raportul privind transparența Google a fost lansat** pentru a arăta cum politicile și acțiunile autorităților guvernamentale și ale entităților corporative afectează confidențialitatea, securitatea și accesul la informații online. În 2018, am adăugat un raport privind transparența specific pentru Android.

2017 – **A fost lansată protecția Google Play**, care în prezent este cea mai larg răspândită soluție de scanare anti-malware pentru peste 125 de miliarde de aplicații instalate pe 3+ miliarde de dispozitive.

2019 – **A fost introdusă cheia de securitate** ca o funcție încorporată pe Android și apoi pentru iPhone, în 2020.

2022 – **Google Play a lansat** o secțiune despre siguranța datelor, pentru a le oferi oamenilor mai multe informații despre cum aplicațiile colectează, distribuie și securizează datele utilizatorilor și a inițiat primul sistem de ecusoane pentru orice aplicație care a trecut printr-o evaluare de securitate independentă, prin Alianța pentru Protecția Aplicațiilor.

2023 – **Codul de acces: viitorul fără parole** este pus în mișcare prin asistență extinsă pentru codurile de acces după un deceniu de încurajare a standardelor deschise prin intermediul Alianței FIDO și al liderilor din domeniul tehnologic din lumea întreagă.

Abordarea noastră

Angajamentul pentru o lume digitală deschisă, securizată

Preocupările de securitate nu vor face decât să crească pentru că din ce în ce mai multe date sunt utilizate pe din ce în ce mai multe dispozitive din rețele diferite. Participăm la evoluția spre un viitor al securității dispozitivelor conectate prin dezvoltarea produselor noastre, criteriile de transparență și parteneriatele din industrie

O piatră de temelie a strategiei noastre pentru produse este asigurarea securității implicite a dispozitivelor noastre. Navigarea sigură, Google Play Protect și Cheile de securitate încorporate protejează dispozitivele mobile și aplicațiile, pentru a oferi produselor noastre un nivel de securitate mai ridicat.

Ajutăm la democratizarea operațiunilor de securitate, fiind deschiși și transparenți cu modul în care rezolvăm problemele și partajăm cunoștințele despre securitatea dispozitivelor conectate. Credem că un ecosistem al surselor deschise poate fi mai sigur decât un ecosistem închis, cu ajutorul abordării noastre de securitate în straturi.

Colaborând cu CSA, ADA și GSMA, ne străduim să dezvoltăm o securitate cibernetică de cel mai înalt nivel, pentru un internet și un viitor mai sigure pentru toți.

Suntem hotărâți să ridicăm ștacheta pentru securitatea dispozitivelor conectate și să stabilim standardul pentru un mediu online mai sigur pentru oricine, oriunde. Află mai multe despre progresul înregistrat de Google în domeniul securității dispozitivelor conectate: g.co/connecteddevicesafety

Surse: [1] Raport cibernetic CNBC, 9 ian 2023, [2] Ce este un atac IoT? Secretele securității IoT, 20 iulie 2021