Bezpieczeństwo urządzeń mobilnych, aplikacji i internetu rzeczy

Chronimy dane i urządzenia na całym świecie

W obliczu drastycznego nasilenia się cyberataków sponsorowanych przez władze państwowe i przestępczości internetowej jesteśmy przekonani, że nasze produkty i usługi mogą być przydatne tylko wtedy, gdy będą bezpieczne. Google jeszcze bardziej niż dotychczas skupia się na ochronie ludzi, organizacji i władz państwowych. Dzielimy się swoją specjalistyczną wiedzą, motywujemy społeczeństwo do reagowania na nieustannie zmieniające się czynniki ryzyka w cyberprzestrzeni i stale pracujemy nad poprawą stanu wiedzy w zakresie cyberbezpieczeństwa, by uczynić świat bezpieczniejszym dla wszystkich.

W związku z tym musimy bezwzględnie być zawsze o krok do przodu, wciąż dostosowywać swoje rozwiązania w zakresie bezpieczeństwa, by sprostać narastającym zagrożeniom, szczególnie jeśli chodzi o zabezpieczanie połączonych urządzeń i aplikacji. Dzięki temu konsumenci będą mieli poczucie bezpieczeństwa i będą mogli swobodnie decydować o wyborze urządzeń, z których będą korzystać.

Wyzwanie

Łączność ma swoją cenę

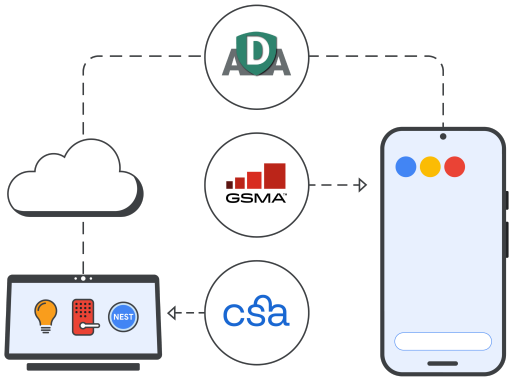
Smartfony, aplikacje i urządzenia IoT są bardzo ważną częścią naszego codziennego życia – spędzamy coraz więcej czasu w internecie i udostępniamy przy tym coraz więcej cennych danych, takich jak dane bankowe czy informacje o zdrowiu. Dlatego wyspecjalizowani cyberprzestępcy coraz częściej atakują te urządzenia, żeby zdobyć wrażliwe informacje.

Więcej urządzeń i danych – więcej zagrożeń

Obecnie na świecie działa około 17 mld urządzeń IoT, od drukarek po sterowniki do bram garażowych. A każde z nich jest wyposażone w oprogramowanie (czasem open source), które można z łatwością zhakować.[1] Liczba urządzeń IoT, w których złamano zabezpieczenia, podwoiła się w 2020 r.[2]

- Choć dzięki urządzeniom IoT stajemy się coraz mocniej skomunikowani, nie istnieją żadne globalne standardy oceny jakości zabezpieczeń produktów podłączonych do internetu. Niedoinformowani, konsumenci mogą przez to podejmować niewłaściwe decyzje dotyczące bezpieczeństwa używanych urządzeń.
- Konsumenci powinni mieć prawo do otrzymywania przejrzystych informacji o posiadanych produktach cyfrowych, analogicznie do prawa wglądu w skład kupowanej żywności czy chemii gospodarczej.
- Urządzenia mobilne otwierają drogę do atakowania innych celów, a ich połączenie sprawia, że rośnie potrzeba udzielania przejrzystych informacji o bezpieczeństwie na masową skalę. To oznacza, że bezpieczeństwo ekosystemu urządzeń połączonych jest równie ważne jak bezpieczeństwo sieci i systemów.

Współpraca z organizacjami branżowymi



Nasze rozwiązanie

Google pracuje nad bezpieczeństwem i przejrzystością urządzeń połączonych, skupiając się na bezpieczeństwie urządzeń mobilnych, aplikacji i internetu rzeczy:

Bezpieczeństwo urządzeń mobilnych

Android, nasz system operacyjny open source, jest wyposażony w wielowarstwowe zabezpieczenia chroniące urządzenia mobilne:

- **Zabezpieczenia wielowarstwowe**
  - Dzięki zabezpieczeniu Verified Boot, ochronie przed przywróceniem starszej wersji systemu (roll-back protection) oraz ochronie przed przywróceniem do ustawień fabrycznych (factory reset protection) użytkownik może zawsze korzystać z najnowszej i najbezpieczniejszej wersji Androida.
  - Kod PIN i uwierzytelnianie biometryczne chronią przed dostępem osób postronnych.
  - „Znajdź moje urządzenie” umożliwia zlokalizowanie skradzionego lub zgubionego urządzenia albo usunięcie jego zawartości.
- **Ochrona tożsamości i ochrona hasłem**
  - Weryfikacja dwuetapowa, telefon jako klucz bezpieczeństwa oraz menedżer haseł chronią Twoje konto Google przed dostępem z zewnątrz.
  - Sprawdzanie zabezpieczeń i opcjonalna Ochrona zaawansowana zapewniają bezpieczne i bezproblemowe działanie urządzenia.
- **Ochrona przed wyłudzaniem informacji**
  - Aplikacje Telefon i Wiadomości Google pomagają wykrywać oszustwa i ataki phishingowe oraz im zapobiegają.
  - Bezpieczne przeglądanie Google chroni ponad 5 miliardów urządzeń na świecie.

Bezpieczeństwo aplikacji

Gotowe do użycia oprogramowanie antymalware stanowi barierę dla złośliwego oprogramowania, a użytkownicy pobierający aplikacje otrzymują przejrzyste informacje o bezpieczeństwie danych.

- Sklep Google Play: Zanim jakiekolwiek aplikacje pojawią się w sklepie, są weryfikowane przez narzędzia uczenia maszynowego do wykrywania zagrożeń, a także przez analityków. W sekcji „Bezpieczeństwo danych” wyjaśniamy, jakie dane są gromadzone przez aplikacje i w jakim celu.
- Google Play Protect: Codziennie skanuje ponad 125 miliardów aplikacji i informuje o wykrytych zagrożeniach lub usuwa aplikacje bądź je wyłącza.
- App Defense Alliance (ADA): Firma Google zawiązała sojusz pod nazwą App Defense Alliance z liderami branży wykrywania zagrożeń dla urządzeń mobilnych, aby chronić użytkowników systemu Android przed potencjalnie szkodliwymi aplikacjami (PHA) poprzez dzielenie się informacjami i koordynację wykrywania zagrożeń.

Bezpieczeństwo internetu rzeczy

Oznakowanie bezpieczeństwa na urządzeniach IoT zawiera dokładne informacje o ochronie prywatności i bezpieczeństwie, na przykład o tym, jakie dane są gromadzone.

- Jeśli chodzi o systemy oznaczania bezpieczeństwa na urządzeniach IoT, kierujemy się pięcioma podstawowymi zasadami: aktualizowanie oznakowania na bieżąco (live label), systemy ocen, standardy bezpieczeństwa (security baselines) połączone z elastycznością, szeroko zakrojona przejrzystość oraz motywowanie do przyjmowania nowych rozwiązań.
- Wspólnie z organizacjami Connectivity Standards Alliance (CSA) i GSM Alliance (GSMA) pracujemy nad standaryzacją branżowego programu certyfikacji pod kątem istniejących i przyszłych wymogów regulacyjnych.

Nasze zasady

W trosce o bezpieczeństwo i przejrzystość skomunikowanych urządzeń Google przestrzega 3 podstawowych zasad:

Dogłębna obrona (Defense in Depth): Korzystamy z wielu różnych warstw architektury bezpieczeństwa, które łącznie zapewniają silną, sprawną i skuteczną obronę.

Otwartość i przejrzystość: Przejrzystość stanowi kluczowy element naszej filozofii. Uważamy, że dzięki przekazywaniu bieżących informacji użytkownikom naszej platformy oraz dzieleniu się wiedzą w celu wzmocnienia ochrony, ekosystem open source może być bezpieczniejszy niż ekosystem zamknięty.

To, co najlepsze w Google i w naszym ekosystemie: Współpracujemy z zespołami ekspertów w Google i w całej branży w trosce o bezpieczeństwo miliardów użytkowników.

Aplikacje

Oznaczenia bezpieczeństwa na urządzeniach IoT: przekazanie kontroli konsumentom

Ponieważ nie istnieje ustalony sposób oznaczania bezpieczeństwa na urządzeniach IoT, nie ma żadnych globalnych standardów, których mogliby przestrzegać producenci tych urządzeń. Użytkownicy również nie otrzymują należnych im informacji o ochronie danych przez urządzenia. Nasza branża musi wspólnie zająć się poprawą bezpieczeństwa urządzeń IoT, aby konsumenci odzyskali poczucie kontroli. Pracujemy nad systemem oznaczania bezpieczeństwa na urządzeniach IoT w ramach swoich wewnętrznych procesów i we współpracy z innymi.

W pierwszej kolejności inwestujemy w zewnętrzne badania nad bezpieczeństwem, które umożliwiają typowanie potencjalnych luk (Google Nest uczestniczy w prowadzonym przez Google programie wykrywania luk Vulnerability Reward Program, który przewiduje nagrody dla osób spoza Google zgłaszających znalezione luki).

Na tej podstawie wydajemy łatki i poprawki dla krytycznych błędów przez co najmniej pięć lat od wprowadzenia produktu na rynek.

Wszystkie nasze urządzenia opracowane od 2019 r. są wyposażone w funkcję Verified Boot, która sprawdza, czy na urządzeniu działają właściwe oprogramowanie i ustawienia ochrony dostępu. Na przykład nasze urządzenia Google Nest są poddawane walidacji w oparciu o uznane w branży zewnętrzne standardy bezpieczeństwa, opracowane m.in. przez ETSI i ISO.

Wraz z naszym bezpiecznym cyklem życia oprogramowania (SDLC) standardy te zmniejszają narażenie konsumentów na niewłaściwe praktyki w obszarze bezpieczeństwa i stanowią krok w kierunku otwartego i bardziej bezpiecznego internetu.

Inwestycje naszej branży i kamienie milowe

2007 Powstało Bezpieczne przeglądanie, które umożliwia proaktywne ostrzeganie użytkowników wchodzących na niebezpieczne strony internetowe i obecnie chroni ponad 5 miliardów urządzeń.

2010 Wydano pierwszy Raport przejrzystości Google, który pokazuje, jak władze państwowe oraz polityka i zasady obowiązujące w przedsiębiorstwach wpływają na ochronę prywatności, bezpieczeństwo i dostęp do informacji w internecie. W 2018 r. wprowadziliśmy oddzielny Raport przejrzystości dotyczący systemu Android.

2017 Uruchomiono Google Play Protect, obecnie najbardziej rozpowszechnione narzędzie do ochrony przed złośliwym oprogramowaniem, które codziennie skanuje ponad 125 miliardów aplikacji na ponad 3 miliardach urządzeń.

2019 Wprowadzono Klucz bezpieczeństwa, wbudowaną funkcję systemu Android, a od 2020 r. również telefonów iPhone.

2022 Google Play uruchomił sekcję dotyczącą bezpieczeństwa danych, zawierającą informacje o gromadzeniu, przekazywaniu i zabezpieczaniu danych użytkowników przez aplikacje. Uruchomiliśmy pionierski system odznak dla aplikacji, które przeszły niezależną weryfikację bezpieczeństwa przez App Defense Alliance.

2023 Klucze: przyszłość bez haseł jest coraz bliżej dzięki rozszerzeniu obsługi kluczy po dziesięciu latach pracy nad otwartymi standardami z FIDO Alliance i światowymi liderami branży technologicznej.

Nasze podejście

Stawiamy na otwarty i bezpieczny cyfrowy świat

Wraz ze wzrostem ilości danych przechowywanych na coraz liczniejszych urządzeniach działających w różnych sieciach obawy o bezpieczeństwo będą oczywiście rosły. Pomagamy kształtować przyszłość bezpieczeństwa połączonych urządzeń dzięki rozwojowi naszych produktów, kryteriom przejrzystości oraz partnerskiej współpracy w obrębie naszej branży.

Podstawą naszej strategii produktowej jest zapewnianie bezpieczeństwa produktów w standardzie. Bezpieczne przeglądanie, Google Play Protect i wbudowane Klucze bezpieczeństwa chronią urządzenia i aplikacje mobilne oraz zapewniają najwyższy poziom bezpieczeństwa naszych produktów.

Staramy się demokratyzować nasze działania w obszarze bezpieczeństwa, w otwarty i przejrzysty sposób informując o rozwiązywaniu problemów oraz dzieląc się wiedzą o bezpieczeństwie urządzeń połączonych. Uważamy, że dzięki naszym wielowarstwowym zabezpieczeniom ekosystem open source może być bezpieczniejszy niż ekosystem zamknięty.

Współpracując z CSA, ADA i GSMA, dążymy do poprawy stanu wiedzy w dziedzinie cyberbezpieczeństwa, by internet i przyszłość były bezpieczniejsze dla wszystkich.

Staramy się stale podnosić standardy bezpieczeństwa urządzeń połączonych i wyznaczamy standard bezpieczniejszego środowiska internetowego dla każdego i wszędzie. Więcej informacji o osiągnięciach Google w obszarze bezpieczeństwa urządzeń połączonych: g.co/connecteddevicesafety

Źródła: [1] CNBC Cyber Report, 9 stycznia 2023 r., [2] What is an IoT Attack? The Ins and Outs of IoT Security, 20 lipca 2021 r.