Безпека мобільних пристроїв, додатків та Інтернету речей

Захист даних і пристроїв у всьому світі

З різким зростанням кількості кібератак і зловмисників в Інтернеті ми вважаємо, що наші продукти й послуги корисні настільки, наскільки вони безпечні. У Google ми як ніколи зосереджені на захисті людей, організацій і урядів. Ми ділимося нашим досвідом, розширюємо можливості суспільства протистояти кіберризикам, що постійно зростають, і працюємо над тим, щоб підняти сучасний рівень кібербезпеки й зробити світ безпечнішим для всіх.

Для нас вкрай важливо діяти на випередження й постійно вдосконалювати наші рішення безпеки, щоб протистояти загрозам, які постійно зростають, особливо коли йдеться про захист усіх підключених пристроїв і програм, і створити для користувачів безпечне середовище, де в них буде впевненість і свобода вибору щодо того, якими пристроями користуватися.

Виклик

Зв'язок має певну ціну

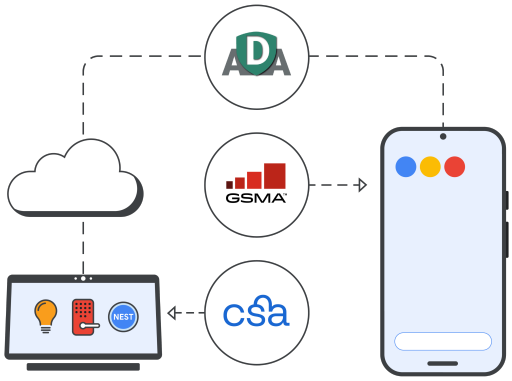
Значну частину нашого повсякденного життя ми проводимо зі смартфонами, додатками й пристроями Інтернету речей, присвячуючи все більше часу Інтернету й обмінюючись при цьому все більшою кількістю цінних даних, таких як банківська або медична інформація. Через це досвідчені кіберзлочинці частіше, ніж будь-коли раніше, націлюються на наші пристрої, щоб отримати конфіденційну інформацію.

Більше пристроїв, більше даних – більше загроз

Зараз у світі налічується приблизно 17 млрд пристроїв Інтернету речей: від принтерів до механізмів відкривання дверей гаража, кожен з яких містить програмне забезпечення (частково з відкритим кодом), яке можна легко зламати.[1] Загалом кількість зламаних пристроїв Інтернету речей збільшилася майже вдвічі у 2020 році.[2]

- Незважаючи на те, що ми все тісніше пов'язані через пристрої Інтернету речей, не існує глобальних стандартів для вимірювання якості безпеки підключених продуктів, через що споживачі приймають несвідомі й необґрунтовані рішення щодо безпеки своїх пристроїв.
- Споживачі повинні мати право знати про ризики, пов'язані з їхніми цифровими продуктами, так само, як вони мають право знати, які складові мають продукти харчування чи миючі засоби, які вони купують.
- Мобільні пристрої – це лише один напрямок атак, а взаємозв'язок між пристроями лише збільшує потребу розуміти ризики безпеки в масштабі. Отже, безпека екосистеми підключених пристроїв така ж важлива, як і безпека мереж і систем.

Наша співпраця з галузевими організаціями



Наше рішення

У Google ми посилюємо захист наших підключених пристроїв і покращуємо прозорість засобів захисту через безпеку мобільних пристроїв, додатків і Інтернету речей:

Безпека мобільних пристроїв

Android, наша операційна система з відкритим вихідним кодом, використовує багаторівневий підхід до безпеки для захисту мобільних пристроїв:

- Багаторівневий захист
  - Завдяки таким функціям, як системи перевірки під час запуску, захист від відкочування до попередньої версії й захист від скидання до заводських налаштувань, користувачі отримують найновішу й найбезпечнішу версію Android.
  - PIN-код і біометрична автентифікація захищають від зовнішнього доступу.
  - Функція пошуку пристрою допомагає знайти пристрій або віддалено стерти на ньому дані, якщо його вкрали чи ви його загубили.
- Захист паролем й ідентифікація
  - Двохетапна перевірка, використання телефона як ключа безпеки й менеджер паролів захищають ваш обліковий запис Google від зовнішнього доступу.
  - Перевірка безпеки й додатковий розширений захист забезпечують захищену й безперебійну роботу пристрою.
- Захист від фішингу
  - Додатки Телефон від Google і Google Повідомлення допомагають виявляти шахрайські й фішингові атаки та запобігати їм.
  - Безпечний перегляд Google захищає понад 5 мільярдів пристроїв у всьому світі.

Безпека додатків

Готові засоби захисту від зловмисного програмного забезпечення запобігають дії шкідливих додатків, а інформація, пов'язана з безпекою даних, допомагає користувачам краще розуміти, як захищаються їхні дані, коли вони завантажують додатки.

- Магазин Google Play: інструменти, що працюють на основі технології машинного навчання, і спеціалісти перевіряють усі додатки, перш ніж вони стануть доступними для завантаження. У розділі "Безпека даних" пояснюється, які типи даних збирають додатки й для чого вони використовуються.
- Google Play Захист: щодня сканує понад 125 мільярдів додатків і сповіщає про виявлені загрози безпеці, а також видаляє або блокує потенційно шкідливі додатки.
- App Defense Alliance (ADA): компанія Google співпрацювала з провідними партнерами з виявлення загроз для мобільних пристроїв, щоб запустити функцію App Defense Alliance, яка допомагає захистити користувачів Android від потенційно шкідливих програм за допомогою спільного й скоординованого аналізу та виявлення вразливостей і загроз.

Безпека Інтернету речей

Мітки безпеки Інтернету речей чітко передають інформацію про методи конфіденційності й безпеки, які застосовуються на пристрої, наприклад, які дані збираються.

- Ми віримо в п'ять основних принципів схем маркування безпеки Інтернету речей: жива мітка, схеми оцінювання, базові рівні безпеки в поєднанні з гнучкістю, широка прозорість та стимули для впровадження.
- Ми співпрацюємо з групою компаній Connectivity Standards Alliance (CSA) і GSM Alliance (GSMA) над стандартизацією загальногалузевої програми сертифікації для існуючих і майбутніх нормативних вимог.

Наші принципи

У Google ми застосовуємо 3 основні принципи для підвищення безпеки та прозорості наших підключених пристроїв:

Поглиблений захист: ми використовуємо кілька рівнів архітектури безпеки, які разом формують надійний захист, що працює гнучко й ефективно.

Відкритість і прозорість: прозорість є ключем до нашої філософії. Інформуючи користувачів нашої платформи й ділячись знаннями для посилення нашого захисту, ми віримо, що екосистема продуктів із відкритим кодом може бути більш безпечною, ніж система із закритим кодом.

Найкраще від Google і нашої екосистеми: ми співпрацюємо з командами експертів із Google та інших компаній у галузі, щоб допомогти захистити мільярди користувачів.

Додатки

Мітки безпеки Інтернету речей: передача контролю в руки споживачів

Без встановлених міток безпеки Інтернету речей не існує глобальних стандартів, яких повинні дотримуватися виробники пристроїв. Користувачі також не мають належної інформації про те, чи пристрої захищають їхні дані. Усі представники галузі мають об'єднатися, щоб посилити безпеку Інтернету речей і повернути контроль у руки споживачів. Ми працюємо над схемою міток безпеки Інтернету речей завдяки нашим процесам і партнерству.

По-перше, ми інвестуємо в дослідження зовнішньої безпеки, щоб точно визначити можливі вразливі місця (Google Nest бере участь у програмі винагород за виявлені вразливі місця Google і винагороджує дослідників безпеки за межами Google, які знаходять вразливості в наших системах).
Після цього ми випускаємо критичні виправлення помилок протягом щонайменше п'яти років після запуску.
Усі наші пристрої, розроблені у 2019 році й пізніше, використовують функцію перевірки системи під час запуску, що забезпечує роботу відповідного програмного забезпечення і захист від стороннього доступу. Наприклад, наші пристрої Google Nest перевіряються за допомогою стандартів безпеки, розроблених іншими представниками галузі, наприклад, організаціями ETSI й ISO.

Ці стандарти й наш безпечний життєвий цикл розробки програмного забезпечення (SDLC) зменшують ймовірність того, що споживачі будуть наражатися на ризик через недієві методи захисту, і відкривають шлях до відкритого, безпечнішого Інтернету.

Наші галузеві інвестиції та віхи

2007 — Запущено Безпечний пошук, який попереджає користувачів, коли вони збираються відкрити небезпечний веб-сайт, і зараз захищає понад 5 мільярдів пристроїв.

2010 — Запущено Звіт Google про доступність сервісів і даних, щоб показати, як правила й дії урядів і компаній впливають на конфіденційність, безпеку й доступ до інформації в Інтернеті. У 2018 році ми додали такий звіт для Android.

2017 — Запущено Google Play Захист, що зараз є найпоширенішим рішенням для захисту від зловмисного програмного забезпечення, яке сканує понад 125 мільярдів додатків на день на більше ніж 3 мільярдах пристроїв.

2019 — Представлено Ключ безпеки як вбудовану функцію для Android, а у 2020 році й для iPhone.

2022 — Google Play запускає розділ "Безпека даних", щоб надати користувачам більше інформації про те, як додатки збирають, обробляють і захищають їхні дані, а також представлено першу систему значків для додатків, які пройшли незалежну перевірку безпеки через ініціативу App Defense Alliance.

2023 — Ключі доступу: майбутнє без паролів розпочинається з розширеної підтримки ключів доступу після десятиліття впровадження відкритих стандартів разом з ініціативою FIDO Alliance і технологічними лідерами з усього світу.

Наш підхід

Прагнення до відкритого, безпечного цифрового світу

Занепокоєння щодо безпеки лише посилюватиметься, оскільки все більше даних буде потрапляти на все більшу кількість пристроїв у різних мережах. Ми допомагаємо наблизити майбутнє, де гарантується безпека підключених пристроїв, розробляючи продукти, критерії прозорості й співпрацюючи з іншими компаніями в галузі.

Наріжним каменем нашої продуктової стратегії є безпека наших продуктів за умовчанням. Безпечний пошук, Google Play Захист і вбудовані ключі безпеки захищають мобільні пристрої і додатки, щоб забезпечити найвищий рівень безпеки в наших продуктах.

Ми допомагаємо демократизувати процеси підвищення безпеки, відкрито ділячись нашими методами вирішення проблем і знаннями про безпеку підключених пристроїв. Ми вважаємо, що екосистема продуктів із відкритим вихідним кодом може бути більш безпечною, ніж закрита екосистема, завдяки нашому багаторівневому підходу до безпеки.

Співпрацюючи з організаціями CSA, ADA і GSMA, ми прагнемо вдосконалювати сучасні технології кібербезпеки для створення безпечнішого Інтернету і майбутнього для всіх.

Ми прагнемо підняти планку безпеки підключених пристроїв і встановити стандарт безпечнішого онлайн-середовища для всіх і всюди. Докладніше про досягнення Google у сфері безпеки підключених пристроїв: g.co/connecteddevicesafety

Джерела: [1] CNBC Cyber Report, 9 січня 2023 року, [2] What is an IoT Attack? The Ins and Outs of IoT Security, 20 липня 2021 року