Bezpečnost mobilních zařízení, aplikací a internetu věcí

Ochrana dat a zařízení po celém světě

Vzhledem k dramatickému nárůstu kybernetických útoků sponzorovaných státy a záškodníků na internetu jsme přesvědčeni, že naše produkty a služby jsou jen tak užitečné, jak jsou bezpečné. Proto se v Googlu nyní víc než dřív zaměřujeme na ochranu lidí, organizací a vlád. Sdílíme své odborné znalosti, pomáháme společnosti čelit neustále se vyvíjejícím kybernetickým rizikům, snažíme se zvyšovat kybernetickou bezpečnost a vytvářet bezpečnější svět pro všechny.

Proto je nezbytné být vždy o krok napřed a neustále vyvíjet bezpečnostní řešení, abychom se uměli vypořádat se stále početnějšími hrozbami, zejména pokud jde o zabezpečení všech připojených zařízení a aplikací, a poskytovali tak spotřebitelům bezpečné prostředí, kde mají možnost volby v zařízeních, s nimiž pracují.

Problém

Daň za konektivitu

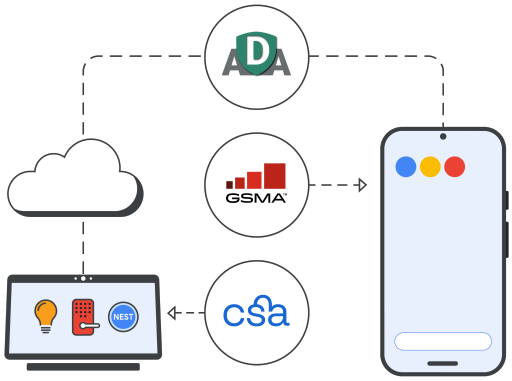
Velkou část každodenního života vedeme prostřednictvím chytrých telefonů, aplikací a zařízení internetu věcí. Trávíme stále více času online a sdílíme přitom stále více cenných údajů, jako jsou bankovní nebo zdravotní informace. Toho umí chytře využít kybernetičtí zločinci, kteří se stále častěji zaměřují na tato zařízení a snaží se z nich získat citlivé údaje.

Více zařízení, více dat – a více hrozeb

Na světě je nyní odhadem 17 miliard zařízení internetu věcí, od tiskáren po otvírače garážových vrat, přičemž každé z nich je vybaveno softwarem (některá s otevřeným zdrojovým kódem), který lze snadno prolomit.[1] Celkově se počet napadených zařízení internetu věcí v roce 2020 téměř zdvojnásobil.[2]

- Přestože jsme prostřednictvím zařízení internetu věcí stále propojenější, globální standardy pro měření kvality zabezpečení připojených produktů neexistují, takže spotřebitelé nemají možnost se informovaně rozhodovat o zabezpečení zařízení.
- Spotřebitelé by měli mít právo na transparentní digitální produkty, podobně jako mají právo vědět, jaké je složení potravin nebo čisticích prostředků, které si kupují.
- Mobilní zařízení jsou jen vstupní branou pro útoky v dalších prostředích, a vzájemné propojení zařízení tak zvyšuje potřebu transparentnosti zabezpečení ve velkém měřítku. Proto je zabezpečení ekosystému propojených zařízení stejně důležité jako zabezpečení sítí a systémů.

Naše spolupráce s oborovými organizacemi



Naše řešení

V Googlu zvyšujeme bezpečnost a transparentnost připojených zařízení prostřednictvím zabezpečení mobilních zařízení, aplikací a internetu věcí:

Bezpečnost mobilních zařízení

Android, náš operační systém s otevřeným zdrojovým kódem, využívá k zabezpečení mobilních zařízení tzv. vrstvený přístup:

- Vrstvené zabezpečení
  - Ověřené spuštění, ochrana proti rollbacku (návratu k předchozí verzi) a ochrana proti obnovení továrního nastavení zajišťují používání nejnovější a nejbezpečnější verze systému Android.
  - Kód PIN a biometrické ověřování chrání před přístupem zvenčí.
  - Funkce „Najdi moje zařízení“ pomáhá lokalizovat zařízení nebo jej vymazat v případě krádeže nebo ztráty.
- Ochrana identity a hesla
  - Dvoufázové ověření, telefon jako bezpečnostní klíč a správce hesel chrání váš účet Google před přístupem zvenčí.
  - Kontrola zabezpečení a volitelná pokročilá ochrana zajišťují bezpečný a bezproblémový provoz zařízení.
- Ochrana proti phishingu
  - Aplikace Telefon od Googlu a Zprávy od Googlu pomáhají odhalovat podvodné a phishingové útoky a předcházet jim.
  - Služba Bezpečné prohlížení Google chrání více než 5 miliard zařízení po celém světě.

Bezpečnost aplikací

Důmyslná ochrana proti malwaru pomáhá blokovat špatné aplikace a informace o bezpečnosti dat poskytují uživatelům transparentnost při stahování aplikací.

- Obchod Google Play: Nástroje pro detekci pomocí strojového učení a lidští analytici kontrolují všechny aplikace předtím, než jsou k dispozici ke stažení. V sekci Zabezpečení údajů je vysvětleno, jaké typy dat aplikace shromažďují a k čemu se tato data používají.
- Google Play Protect: Každý den prohledá více než 125 miliard aplikací, a pokud zjistí bezpečnostní riziko, zašle upozornění a aplikaci odstraní nebo zakáže.
- App Defense Alliance (ADA): Společnost Google ve spolupráci s předními partnery v oblasti detekce mobilních hrozeb založila alianci App Defense Alliance, která pomáhá chránit uživatele systému Android před potenciálně škodlivými aplikacemi (PHA) prostřednictvím sdílených informací a koordinovaného odhalování.

Bezpečnost internetu věcí

Bezpečnostní štítky IoT jasně informují o postupech ochrany soukromí a zabezpečení zařízení, například o tom, jaká data jsou shromažďována.

- Vyznáváme pět základních principů systémů označování bezpečnosti IoT: živé označování, systémy hodnocení, základní bezpečnostní standardy spojené s flexibilitou, širokou transparentnost a pobídky k přijetí.
- Spolupracujeme s aliancemi Connectivity Standards Alliance (CSA) a GSM Alliance (GSMA) na standardizaci certifikačního programu pro stávající a budoucí regulační požadavky, který se bude používat v rámci celého odvětví.

Naše zásady

V Googlu uplatňujeme tři základní zásady pro zvýšení bezpečnosti a transparentnosti našich připojených zařízení:

Hloubková obrana: Využíváme více vrstev bezpečnostní architektury, které společně vytvářejí silnou, bezproblémově a efektivně fungující obranu.

Otevřenost a transparentnost: Transparentnost je základním kamenem naší filosofie. Věříme, že otevřený ekosystém může být bezpečnější než uzavřený. Když tedy informujeme uživatele naší platformy a sdílíme s nimi znalosti, posilujeme naši ochranu.

To nejlepší z Googlu a našeho ekosystému: Spolupracujeme s týmy odborníků z Googlu i celého odvětví, abychom pomohli zajistit bezpečnost miliard uživatelů.

Aplikace

Bezpečnostní štítky internetu věcí: kontrola v rukou spotřebitelů

Dosud nebylo zavedeno bezpečnostní značení internetu věcí, neexistují tedy žádné globální normy, kterými by se výrobci zařízení mohli řídit. Uživatelé tak nemají zasloužený přehled o tom, zda jejich zařízení chrání jejich data. Celé odvětví se proto musí spojit v úsilí posunout bezpečnost internetu věcí kupředu a vrátit kontrolu do rukou spotřebitelů. My se prostřednictvím našich procesů a partnerství snažíme dosáhnout toho, aby se systém bezpečnostního značení internetu věcí už brzy mohl zavést.

V první řadě investujeme do externího bezpečnostního výzkumu, abychom odhalili možné zranitelnosti (Google Nest se účastní programu odměn za odhalování chyb v zabezpečení Google a odměňuje výzkumníky mimo Google, kteří hledají bezpečnostní chyby).
Dále vydáváme záplaty a opravy kritických chyb po dobu nejméně pěti let od vydání.
Všechna naše zařízení vyvinutá v roce 2019 a později používají Verified Boot, systém ověřeného spuštění, který zajistí spuštění správného softwaru a ochranu přístupu. Například naše zařízení Google Nest se validují pomocí uznávaných bezpečnostních standardů třetích stran, jako jsou ETSI a ISO.

Tyto standardy a náš bezpečný životní cyklus vývoje softwaru (SDLC) snižují pravděpodobnost, že spotřebitelé budou vystaveni špatným bezpečnostním praktikám, a připravují půdu pro otevřený a bezpečnější internet.

Naše investice a milníky v oboru

2007 Zavedení bezpečného prohlížení Safe Browsing, které proaktivně upozorňuje uživatele při návštěvě nebezpečných webových stránek a nyní chrání více než 5 miliard zařízení.

2010 Spuštění webu Google Transparency Report, který zveřejňuje údaje o tom, jak předpisy a opatření úřadů státní správy a společností ovlivňují soukromí, bezpečnost a přístup k informacím na internetu. V roce 2018 jsme přidali verzi Transparency Report určenou pro systém Android.

2017 Spuštění služby Google Play Protect, která je nyní nejrozšířenějším řešením proti malwaru a denně kontroluje více než 125 miliard aplikací ve více než 3 miliardách zařízení.

2019 Představili jsme bezpečnostní klíč jako integrovanou funkci pro Android a v roce 2020 i pro iPhone.

2022 Google Play spustil sekci Zabezpečení údajů, která lidem poskytne více informací o tom, jak aplikace shromažďují, sdílejí a zabezpečují data uživatelů, a první systém odznaků pro všechny aplikace, které prošly nezávislou bezpečnostní kontrolou App Defense Alliance.

2023 Přístupový klíč: budoucnost bez hesel. Po deseti letech prosazování otevřených standardů s aliancí FIDO a technologickými lídry po celém světě se dává do pohybu rozšířená podpora přístupových klíčů.

Náš přístup

Odhodlání budovat otevřený a bezpečný digitální svět

S větším množstvím dat na více zařízeních v různých sítích se budou dále zvyšovat obavy o bezpečnost. Vývojem produktů a rozvojem kritérií transparentnosti a průmyslových partnerství chceme prosazovat lepší budoucnost v oblasti zabezpečení připojených zařízení.

Základem naší produktové strategie je zajištění výchozího zabezpečení našich produktů. Funkce Bezpečné prohlížení, Google Play Protect a integrované bezpečnostní klíče chrání mobilní zařízení a aplikace a poskytují nejvyšší úroveň zabezpečení našich produktů.

Jsme otevření a transparentní při řešení problémů a sdílení znalostí o zabezpečení připojených zařízení, čímž pomáháme demokratizovat bezpečnostní operace. Věříme, že ekosystém s otevřeným zdrojovým kódem může být díky našemu vrstvenému přístupu k zabezpečení bezpečnější než uzavřený ekosystém.

Spoluprací s CSA, ADA a GSMA usilujeme o pokrok v oblasti kybernetické bezpečnosti pro bezpečnější internet a budoucnost pro všechny.

Jsme odhodláni zvyšovat laťku zabezpečení připojených zařízení a nastavit standard pro bezpečnější online prostředí pro všechny a všude. Přečtěte si více o pokroku společnosti Google v oblasti zabezpečení připojených zařízení: g.co/connecteddevicesafety

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