Mobiele, app-, en IoT beveiliging

Wereldwijd beschermen van gegevens en apparatuur

Met de extreme toename van staatsgesponsorde hackersaanvallen en kwaadwillende individuen online, vinden we dat onze producten en diensten alleen nuttig zijn als ze echt veilig zijn. Bij Google zijn we er meer dan ooit op gericht mensen, organisaties en overheden te **beschermen** door onze expertise te delen, de samenleving **de middelen te geven** om de steeds evoluerende digitale risico's aan te pakken en zich voortdurend in te zetten voor de bescherming van mensen en overheden, en voortdurend te werken aan de **verbetering** van de stand van de techniek op het gebied van cybersecurity om zo een veiligere wereld voor iedereen te realiseren.

Daarom is het voor ons noodzaak om de ontwikkelingen voor te blijven en onze beveiligingsoplossingen voortdurend te ontwikkelen om het steeds maar groeiende bedreigingslandschap aan te pakken, met name als het gaat om de beveiliging van alle verbonden apparaten en apps. Zo kunnen we consumenten een veilige omgeving bieden waarin ze zelf kunnen bepalen met welke apparaten ze aan de slag gaan.

Uitdaging

Aan connectiviteit hangt wel een prijskaartje

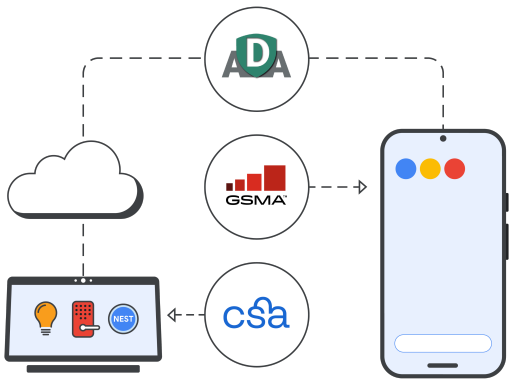
We brengen zo veel van ons dagelijks leven door op onze smartphones, apps en IoT-apparaten – we brengen steeds meer tijd online door en daarbij delen we steeds meer waardevolle gegevens, zoals bank- of gezondheidszorggegevens. Daarom richten geraffineerde cybercriminelen zich meer dan ooit op deze apparaten om gevoelige gegevens te bemachtigen.

Meer apparaten, meer gegevens, meer dreigingen

Wereldwijd zijn er nu naar schatting 17 miljard IoT-apparaten, van printers tot garagedeuropeners, en stuk voor stuk zitten ze vol met (deels open-source-) software die gemakkelijk gehackt kan worden.[1] Het totale aantal gehackte IoT-apparaten was bijna verdubbeld in 2020.[2]

- Hoewel we via IoT-apparaten steeds nauwer met elkaar verbonden raken, zijn er geen wereldwijde normen voor het meten van de beveiligingskwaliteit van met elkaar verbonden producten, waardoor consumenten ongeïnformeerde beslissingen over de beveiliging van apparaten moeten maken.
- Consumenten behoren het recht te hebben op transparantie omtrent hun digitale producten, net zoals ze het recht hebben om te weten welke bestanddelen er in het voedsel of de schoonmaakmiddelen zitten die ze kopen.
- Mobiele apparaten zijn maar één vector voor verschillende aanvalsterreinen, maar door de interconnectiviteit van apparaten neemt de behoefte aan beveiligingstransparantie op schaal toe. Daarom is de beveiliging van het ecosysteem van onderling verbonden apparaten even belangrijk als de beveiliging van netwerken en systemen.

Onze samenwerking met brancheorganisaties



Onze oplossing

Bij Google bevorderen we de beveiliging en transparantie van onze internetapparaten door middel van mobiele, app- en IoT-beveiliging:

Mobiele veiligheid

Android, ons opensourcebesturingssysteem, maakt gebruik van een gelaagde beveiligingsaanpak waarmee mobiele apparaten veilig worden gehouden:

- Gelaagde beveiliging
  - Verified Boot, rollbackbescherming en fabrieksresetbescherming zorgen voor de nieuwste, veiligste Android-versie.
  - Pincode en biometrische identificatie beschermen tegen toegang van buitenaf.
  - 'Vind mijn apparaat' helpt het apparaat te vinden of te wissen als het gestolen of verloren is.
- Identiteits- en wachtwoordbeveiliging
  - Verificatie in twee stappen, je telefoon als beveiligingssleutel en wachtwoordmanager beschermen je Google-account tegen toegang van buitenaf.
  - Beveiligingscontrole en optionele geavanceerde beveiliging zorgen ervoor dat het apparaat veilig en probleemloos blijft werken.
- Bescherming tegen phishing
  - Phone by Google en Messages by Google helpen bij het detecteren en voorkomen van scam- en phishing-aanvallen.
  - Google Safe Browsing houdt wereldwijd meer dan 5 miljard apparaten veilig.

Beveiliging van apps

De kant-en-klare anti-malware helpt schadelijke apps buiten de deur te houden en informatie over gegevensveiligheid biedt gebruikers transparantie wanneer ze apps downloaden.

- Google Play Store: Alle apps worden door machinelearning-detectietools en menselijke analisten beoordeeld voordat ze kunnen worden gedownload. Het gedeelte over gegevensveiligheid legt uit welke soorten gegevens door apps worden verzameld en waarvoor die gegevens worden gebruikt.
- Google Play Protect: Scant elke dag meer dan 125 miljard apps en waarschuwt, verwijdert of deactiveert ze als er beveiligingsrisico's worden gedetecteerd.
- App Defense Alliance (ADA): Google werkte samen met de toonaangevende partners op het gebied van detectie van mobiele bedreigingen en introduceerde de Defense Alliance-app, die Android-gebruikers door middel van gedeelde informatie en gecoördineerde detectie helpt beschermen tegen potentieel schadelijke toepassingen (PHA's).

IoT-beveiliging

IoT-beveiligingslabels geven duidelijk aan wat de privacy- en beveiligingspraktijken zijn van een apparaat, zoals welke gegevens worden verzameld.

- Volgens ons zijn er vijf kernbeginselen voor IoT-beveiligingslabelschema's: live-labels, evaluatieschema's, beveiligingsgrondbeginselen gekoppeld aan flexibiliteit, brede transparantie en aanmoedigingen voor invoering.
- Samen met de Connectivity Standards Alliance (CSA) en de GSM Alliance (GSMA) werken we aan de standaardisering van een certificeringsprogramma voor de hele branche voor bestaande en toekomstige wettelijke vereisten.

Onze principes

Bij Google passen we 3 kernprincipes toe om de beveiliging en transparantie van onze onderling verbonden apparaten te bevorderen:

Diepgaande bescherming: We gebruiken beveiligingsarchitectuur met meerdere lagen die samenwerken om een sterke bescherming op te bouwen die soepel en effectief werkt.

Open en transparant: Transparantie vormt de kern van onze filosofie. Doordat we de gebruikers van ons platform op de hoogte houden en kennis delen om onze beveiliging te versterken, geloven we dat een open source ecosysteem veiliger kan zijn dan een gesloten systeem.

Het beste van Google en ons ecosysteem: We werken samen met deskundige teams bij Google en uit de branche om miljarden gebruikers veilig te houden.

Toepassingen

IoT-beveiligingslabels: de regie bij de consument leggen

Zonder vastgestelde IoT-beveiligingslabels zijn er geen wereldwijde normen die fabrikanten van apparaten kunnen volgen. Ook hebben gebruikers niet het overzicht dat ze verdienen met betrekking tot de vraag of hun apparaten hun gegevens beschermen. De branche moet de handen ineenslaan om IoT-beveiliging te bevorderen en de regie weer bij de consument te leggen. Met onze processen en partnerschappen werken we aan een IoT-veiligheidslabel.

Om te beginnen investeren we in extern beveiligingsonderzoek om mogelijke kwetsbaarheden op te sporen (Google Nest neemt deel aan het beloningsprogramma voor kwetsbaarheden van Google en beloont beveiligingsonderzoekers buiten Google die kwetsbaarheden vinden).
Van daaruit geven we kritische bugpatches en -fixes uit gedurende ten minste vijf jaar na de introductie.
Al onze apparaten die vanaf 2019 zijn ontwikkeld, maken gebruik van Verified Boot, wat ervoor zorgt dat de juiste software wordt gedraaid en de toegang wordt beveiligd. Onze Google Nest-apparaten zijn bijvoorbeeld gevalideerd aan de hand van door de branche erkende beveiligingsnormen van derden, zoals de standaarden die door ETSI en ISO zijn ontwikkeld.

In combinatie met onze veilige Software Development Life Cycle (SDLC) verkleinen deze normen de kans dat consumenten worden blootgesteld aan gebrekkige beveiligingspraktijken en maken de weg vrij voor een open en veiliger internet.

Onze branche-investeringen en mijlpalen

2007 — **Safe Browsing begon met het** proactief waarschuwen van gebruikers wanneer ze gevaarlijke websites bezoeken en beschermt nu meer dan 5 miljard apparaten.

2010 — **Uitbrengen van het Google Transparency Report** om te laten zien hoe beleid en optreden van overheden en bedrijven invloed hebben op de privacy, veiligheid en toegang tot informatie online. In 2018 hebben we een Android-specifiek transparantierapport toegevoegd.

2017 — **Introductie van Google Play Protect** nu de meest gebruikte antimalwareoplossing die meer dan 125 miljard apps per dag scant op meer dan 3 miljard apparaten.

2019 — **Invoering van de beveiligingssleutel** als ingebouwde functie op Android en vervolgens voor de iPhone in 2020.

2022 — **Google Play introduceerde** een sectie over gegevensveiligheid om mensen meer informatie te geven over hoe apps gegevens van gebruikers verzamelen, delen en beveiligen. Ook heeft Google Play het eerste systeem van badges geïntroduceerd voor apps die via de App Defense Alliance een onafhankelijke veiligheidsbeoordeling hebben ondergaan.

2023 — **Passkey: de wachtwoordloze toekomst** wordt in gang gezet met uitgebreide passkey-ondersteuning na tien jaar een drijvende kracht te zijn geweest achter open standaarden met de FIDO Alliance en techleiders wereldwijd.

Onze aanpak

Inzet voor een open, veilige digitale wereld

De zorgen over de beveiliging zullen alleen maar toenemen naarmate er steeds meer gegevens op steeds meer apparaten staan in verschillende netwerken. Door onze productontwikkeling, transparantiecriteria en samenwerkingsverbanden met de branche helpen we de toekomst van de beveiliging van onderling verbonden apparaten vooruit

Een hoeksteen van onze productstrategie is ervoor zorgen dat onze producten standaard veilig zijn. Safe Browsing, Google Play Protect en ingebouwde beveiligingssleutels bieden bescherming van mobiele apparaten en apps met het hoogste beveiligingsniveau voor onze producten.

Door open en transparant te zijn in de manier waarop we problemen aanpakken en kennis over de beveiliging van onderling verbonden apparaten te delen, helpen we beveiligingsactiviteiten te democratiseren. We geloven dat een opensource-ecosysteem met onze gelaagde beveiligingsaanpak veiliger kan zijn dan een gesloten ecosysteem.

Door samenwerking binnen CSA, ADA en GSMA streven we ernaar de stand van de techniek op het gebied van cyberbeveiliging te verbeteren voor een veiliger internet en een veiligere toekomst voor iedereen.

Ons streven is om de lat voor de beveiliging van onderling verbonden apparaten hoger te leggen en de norm te stellen voor een veiligere online omgeving voor iedereen, overal. Meer informatie over de vorderingen van Google's beveiliging van aangesloten apparaten: g.co/connecteddevicesafety

Bronnen: [1] CNBC Cyber Report, 9 jan 2023, [2] What is an IoT Attack? The Ins and Outs of IoT Security, 20 juli 2021