Sicherheit für Mobilgeräte und IoT

Schutz für Daten und Geräte – weltweit

Angesichts der rasanten Zunahme staatlich geförderter Cyberangriffe und böswilliger Akteure im Internet sind wir bei Google davon überzeugt, dass unsere Produkte und Dienstleistungen sicher sein müssen, damit sie den Menschen helfen. Unser Fokus liegt mehr denn je darauf, Gesellschaft, Wirtschaft, Staat und Verwaltung zu schützen, indem wir unser Fachwissen weitergeben und alle Menschen dabei unterstützen, mit den sich ständig weiterentwickelnden Cyberbedrohungen umzugehen. Wir arbeiten kontinuierlich daran, den Fortschritt der Technik im Bereich Onlinesicherheit voranzutreiben, um unsere Gesellschaft ein Stück weit sicherer zu machen.

Es ist uns sehr wichtig, stets auf neue Entwicklungen zu reagieren und unsere Sicherheitslösungen ständig weiterzuentwickeln. Nur so können wir den zunehmenden Bedrohungen begegnen – insbesondere, wenn es um den Schutz von vernetzten Geräten und Apps geht. Unser Ziel ist es, Menschen ein sicheres Umfeld zu bieten, in dem sie selbst über die Nutzung und Verwaltung ihrer Geräte bestimmen können.

Die Herausforderung

Konnektivität hat ihren Preis

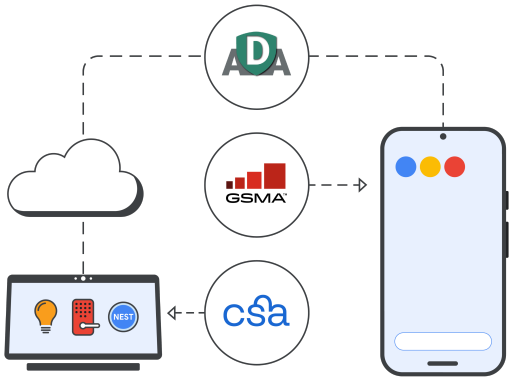
Einen Großteil unseres Alltags verbringen wir mit unseren Smartphones, in Apps und mit IoT-Geräten. Wir erledigen immer mehr online und teilen dabei auch sensible Daten wie Bank- oder Gesundheitsinformationen. Aus diesem Grund werden unsere im Alltag oft verwendeten Geräte vermehrt zum Ziel von Angriffen durch hochspezialisierte Cyberkriminelle, die es genau auf diese vertraulichen Daten abgesehen haben.

Mehr Geräte, mehr Daten – mehr Bedrohungen

Weltweit gibt es mittlerweile schätzungsweise 17 Milliarden IoT-Geräte – vom Drucker bis zum Garagentoröffner. Alle funktionieren mittels Software (darunter auch Open Source), die leicht gehackt werden kann.[1] Die Gesamtanzahl der kompromittierten IoT-Geräte hat sich im Jahr 2020 nahezu verdoppelt.[2]

- Auch wenn wir durch IoT-Geräte immer stärker vernetzt sind, gibt es noch keine globalen Standards zur Messung der Sicherheitsqualität von vernetzten Produkten. Das führt dazu, dass Nutzer:innen oft nicht über die notwendigen Informationen verfügen, um beim Thema Gerätesicherheit die richtigen Entscheidungen zu treffen.
- Nutzer:innen sollten bei digitalen Produkten einen Anspruch auf Transparenz haben – ähnlich wie sie ein Recht haben, zu wissen, welche Inhaltsstoffe in ihren Lebensmitteln oder Reinigungsprodukten enthalten sind.
- Mobilgeräte sind nur ein Einfallstor, über das weitere Angriffsflächen entstehen können. Die Interkonnektivität von Geräten erhöht die Notwendigkeit einer umfassenden Transparenz beim Thema Sicherheit. Deshalb ist der Schutz vernetzter Geräte ebenso wichtig wie die Sicherheit von Netzwerken und Systemen.

Unsere Zusammenarbeit mit Branchenpartnern



Unsere Lösung

Unser Ansatz für mehr Sicherheit und Transparenz bei vernetzten Geräten besteht in umfassenden Sicherheitsfunktionen für Apps, IoT-Geräte und Mobilgeräte:

Sicherheit von Mobilgeräten

Mit Android, unserem Open-Source-Betriebssystem, werden Mobilgeräte durch ein mehrstufiges Sicherheitskonzept geschützt:

- **Mehrstufige Sicherheit**
  - Der verifizierte Bootmodus sowie der Rollback-Schutz ermöglichen es Nutzer:innen, eine sichere Android-Version zu nutzen.
  - PIN und biometrische Authentifizierung schützen vor unberechtigten Zugriffen.
  - „Mein Gerät finden“ hilft, ein Gerät zu lokalisieren oder seine Inhalte zu löschen, wenn es gestohlen oder verloren wurde.
- **Identitäts- und Passwortschutz**
  - Die 2-Faktor-Authentifizierung, das Smartphone als Sicherheitsschlüssel und der Passwortmanager schützen Google-Konten vor unberechtigten Zugriffen.
  - Der Sicherheitscheck und das erweiterte Sicherheitsprogramm sorgen dafür, dass das Gerät geschützt wird.
- **Schutz vor Phishing-Angriffen**
  - Die Telefon App von Google und Messages von Google helfen dabei, Betrugs- und Phishing-Versuche zu erkennen.
  - Google Safe Browsing schützt bereits über 5 Milliarden Geräte weltweit.

App Security

Mit dem Malware-Schutz können schädliche Apps ferngehalten werden. Beim Herunterladen von Apps sorgen Hinweise zur Datensicherheit für mehr Transparenz.

- Google Play Store: Bevor eine App zum Download bereitgestellt wird, wird sie durch Machine-Learning-Erkennungstools und menschliche Analysten überprüft. Im Abschnitt zur Datensicherheit wird erläutert, welche Daten Apps erheben und wofür diese verwendet werden.
- Google Play Protect: Scannt täglich mehr als 125 Milliarden Apps. Wenn dabei Sicherheitsrisiken erkannt werden, erhalten Nutzer:innen eine Benachrichtigung. So können schädliche Apps auf Ihrem Gerät deaktiviert oder entfernt werden.
- App Defense Alliance (ADA): Google hat zusammen mit führenden Branchenpartnern im Bereich Bedrohungserkennung für Mobilgeräte die App Defense Alliance gegründet. Bei dieser Kooperation werden Informationen ausgetauscht und die Erkennung potenziell schädlicher Anwendungen (PSA) koordiniert, um Android-Nutzer besser zu schützen.

IoT-Sicherheit

IoT-Sicherheitskennzeichnungen informieren über Datenschutz- und Sicherheitsfunktionen eines Geräts, z. B. darüber, welche Daten erhoben werden.

- Wir glauben an die fünf Grundsätze der IoT-Sicherheitskennzeichnung: Kennzeichnung in Echtzeit, Bewertungssysteme, flexibel erweiterbare Sicherheitsrichtlinien, breit angelegte Transparenz und Anreize zur Einführung.
- Gemeinsam mit der Connectivity Standards Alliance (CSA) und der GSM Alliance (GSMA) arbeiten wir an einem standardisierten branchenweiten Zertifizierungsprogramm für bestehende und künftige regulatorische Anforderungen.

Unsere Leitlinien

Bei unserem Ansatz zur Verbesserung der Sicherheit und Transparenz vernetzter Geräte richten wir uns nach drei Grundprinzipien:

Umfassender Schutz: Die verschiedenen Stufen unserer Sicherheitsinfrastruktur bilden zusammen eine leistungsstarke Abwehr, die reibungslos und effektiv funktioniert.

Offen und transparent: Unsere Philosophie basiert auf Transparenz. Wir sind der Überzeugung, dass gerade die Offenheit des Open-Source-Ansatzes das ganze Ökosystem sicherer macht. Um einen bestmöglichen Schutz zu bieten, teilen wir unser Wissen regelmäßig mit den Nutzer:innen unserer Plattformen.

Das Beste von Google und darüber hinaus: Gemeinsam mit unseren Branchenpartnern schützen unsere Google-Expertenteams Milliarden von Nutzer:innen.

Anwendungen

IoT-Sicherheitskennzeichnungen: Mehr Transparenz für Nutzer:innen

Ohne anerkannte IoT-Sicherheitskennzeichnungen gibt es keine globalen Standards, denen Geräteheersteller folgen können. Nur wenn Nutzer:innen ausreichend informiert werden, können Sie z. B. beurteilen, ob Geräte ihre Daten schützen. Die Branche muss sich zusammenschließen, um IoT-Geräte sicherer zu machen und den Verbraucher:innen informierte Entscheidungen zu ermöglichen. In unseren Prozessen und Partnerschaften arbeiten wir auf ein einheitliches System für IoT-Sicherheitskennzeichnung hin.

Wir investieren auch in die Sicherheitsforschung mit externen Partnern, um mögliche Schwachstellen zu lokalisieren (Ein Beispiel: Google Nest ist Teil des Google Vulnerability Reward Program und bietet Belohnungen für Sicherheitsforscher:innen außerhalb von Google, die Schwachstellen offenlegen).

Auf dieser Grundlage veröffentlichen wir für mindestens fünf Jahre nach dem Release eines Produkts auf dem amerikanischen Markt kritische Fehlerbehebungen und -korrekturen.

Alle unsere ab 2019 entwickelten Geräte nutzen den verifizierten Bootmodus. Die Sicherheitsfunktion sorgt dafür, dass die richtige Software ausgeführt wird und der Zugriff geschützt ist. So werden unsere Google Nest-Geräte anhand von branchenweit anerkannten Sicherheitsstandards von Drittanbietern validiert, wie beispielsweise denen von ETSI und ISO.

Mithilfe dieser Standards und unserem Qualitätssicherungsprozess bei der Softwareentwicklung (Software Development Life Cycle – SDLC) verringern wir das Risiko, dass Nutzer:innen unzureichenden Sicherheitsstandards ausgesetzt werden. So leisten wir unseren Beitrag zu einem offenen und sichereren Internet für alle.

Unsere Meilensteine und Investitionen in die Branche

2007 – **Start von Safe Browsing.** Nutzer:innen werden proaktiv vor gefährlichen Websites gewarnt. Die Funktion schützt mehr als 5 Milliarden Geräte.

2010 – **Veröffentlichung Google Transparenzbericht.** Der Bericht zeigt auf, wie sich Richtlinien und Maßnahmen von Behörden und Unternehmen auf Datenschutz, Sicherheit und den Zugriff auf Informationen im Internet auswirken. In 2018 haben wir einen Android-spezifischen Transparenzbericht veröffentlicht.

2017 – **Launch von Google Play Protect.** Die heute am häufigsten eingesetzte Anti-Malware-Lösung scannt täglich über 125 Milliarden Apps auf mehr als 3 Milliarden Geräten.

2019 – **Einführung Sicherheitsschlüssel.** Integrierte Funktion für Android, seit 2020 auch für das iPhone.

2022 – **Google Play führt den Abschnitt zur Datensicherheit ein.** Nutzer:innen können so vor der Installation einer App ausführliche Informationen darüber erhalten, wie diese ihre Daten erhebt, weitergibt und schützt. Außerdem startete Google Play das erste Badge-System für Apps, die eine unabhängige Sicherheitsüberprüfung durch die App „Defense Alliance“ durchlaufen haben.

2023 – **Passkey: Die passwortlose Zukunft.** Beginnt mit erweiterter Passkey-Unterstützung, nachdem ein Jahrzehnt lang offene Standards mit der FIDO Alliance und globalen Technologieführern vorangetrieben wurden.

Unser Ansatz

Für ein offenes und vertrauenswürdiges Internet

Mit immer größeren Datenmengen auf immer mehr Geräten in verschiedenen Netzwerken werden auch die Sicherheitsbedenken immer weiter zunehmen. Wir möchten unseren Teil dazu beitragen, vernetzte Geräte sicherer zu machen – durch unsere Produktentwicklungen, unsere Kriterien für mehr Transparenz und unsere Partnerschaften in der Branche.

Ein Kernziel unserer Produktstrategie ist die Entwicklung von Produkten mit integrierten Sicherheitsfunktionen. Durch Safe Browsing, Google Play Protect und integrierte Sicherheitsschlüssel werden Mobilgeräte und Apps geschützt.

Wir tragen dazu bei, Sicherheitsabläufe für alle verständlich und zugänglich zu machen – indem wir Herausforderungen offen und transparent angehen und unser Wissen über die Sicherheit vernetzter Geräte teilen. Wir sind der Überzeugung, dass ein offener Open-Source-Ansatz mit unserem mehrstufigen Sicherheitskonzept sicherer sein kann als ein geschlossenes System.

Im Rahmen unserer Zusammenarbeit mit CSA, ADA und GSMA setzen wir uns dafür ein, den Stand der Technik im Bereich der Cybersecurity voranzutreiben, um Menschen weltweit bestmöglich zu schützen.

Wir setzen uns dafür ein, die Sicherheitsstandards für vernetzte Geräte zu erhöhen und somit das Internet für alle sicherer zu machen. Unter g.co/connecteddevicesafety erfahren Sie, wie Google die Sicherheit verbundener Geräte vorantreibt.

Quellen: 1 CNBC Cyber Report, 9. Januar 2023, 2 What is an IoT Attack? The Ins and Outs of IoT Security, 20. Juli 2021