Mobil, Uygulama ve IoT Güvenliği

Dünyanın her yerinde verileri ve cihazları koruyoruz

Devlet destekli siber saldırılar ve çevrimiçi kötü amaçlı aktörlerin sayısında görülen önemli artışla birlikte ürün ve hizmetlerimizin faydalı olmalarının yanı sıra güvenli olmaları gerektiğine de inanıyoruz. Google olarak; uzmanlığımızı paylaşarak, sürekli değişen siber riskleri ele almak için toplumu güçlendirerek ve herkes için daha güvenli bir dünya inşa etme amacıyla en son siber güvenlik teknolojisinde ilerleme sağlamak için sürekli çalışarak insanları, kuruluşları ve devletleri korumaya her zamankinden daha çok odaklanıyoruz.

Bu sebeple, bir adım önde olup durmadan büyüyen tehdit ortamıyla mücadele etmek için güvenlik çözümlerimizi sürekli olarak geliştirmemiz gerekiyor. Bu durum, tüketicilere etkileşimde bulundukları cihazlarda temsilci ve seçim hakkına sahip oldukları güvenli bir ortam sağlamak için, özellikle bağlı tüm cihazların ve uygulamaların korunmasıyla ilgili olarak daha da önemlidir.

Zorluk

Bağlantının bir bedeli var

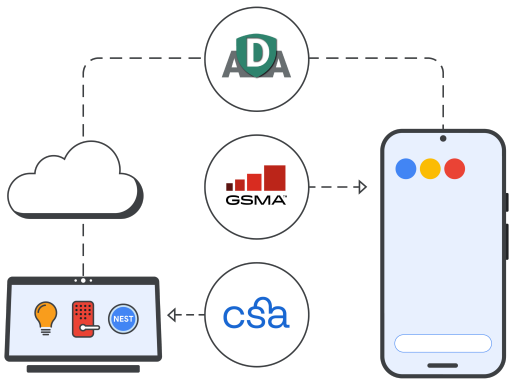
Günlük yaşamımızın büyük bir bölümünü akıllı telefonlar, uygulamalar ve IoT cihazlarıyla yönetiyoruz; daha çok çevrimiçi zaman harcıyoruz ve bu süreçte bankacılık ya da sağlık bilgileri gibi daha çok değerli bilgiyi paylaşıyoruz. Bu sebepten dolayı, sofistike siber suçlular hassas bilgileri elde etmek amacıyla bu cihazları her zamankinden daha çok hedef alıyorlar.

Daha fazla cihaz, daha fazla veri ve daha fazla tehdit

Bugün dünyada, her biri kolayca hacklenebilecek (bazıları açık kaynak) yazılım kurulu olan, yazıcılardan garaj kapısı kumandalarına kadar 117 milyar adet IoT cihazı olduğu tahmin ediliyor.[1] Genel olarak, risk altındaki IoT cihazlarının sayısı 2020 yılında neredeyse iki katına çıktı.[2]

- IoT cihazları aracılığıyla oldukça bağlı hâle gelmemize rağmen bağlı ürünlerin güvenlik kalitesini ölçmek için küresel standartlar yok ve bu durum tüketicilerin cihaz güvenliği konusunda bilgilendirilmemiş kararlar almalarına sebep oluyor.
- Tüketiciler, satın aldıkları yiyeceklerin veya temizlik ürünlerinin içinde neler olduğunu bilme hakkına sahip oldukları gibi dijital ürünleriyle ilgili şeffaflık hakkına da sahip olmalılar.
- Mobil cihazlar diğer saldırı yüzeyleri için sadece bir vektör işlevi görür ve cihazların birbiriyle bağlanabilirliği, ölçeklenebilir güvenlik şeffaflığına olan ihtiyacı artıran bir etken. Dolayısıyla, bağlı cihaz ekosisteminin güvenliği, ağların ve sistemlerin güvenliği kadar önemlidir.

Sektör kuruluşlarıyla iş birliğimiz



Çözümümüz

Google olarak, bağlı cihazlarımızın güvenliğini ve şeffaflığını mobil, uygulama ve IoT güvenliği aracılığıyla artırıyoruz:

Mobil Güvenlik

Açık kaynak işletim sistemimiz olan Android, mobil cihazların güvenliğini sağlamak için katmanlı bir güvenlik yaklaşımından faydalanır.

- Katmanlı Güvenlik
  - Doğrulanmış Başlatma, geriye alma koruması ve fabrika ayarlarına sıfırlama koruması, en güncel ve en güvenli Android sürümünün sunulmasını sağlar.
  - Dışarıdan erişime karşı PIN ve biyometrik doğrulama kalkanı.
  - 'Cihazımı Bul' özelliği cihazı bulmaya ya da cihaz çalınmış veya kaybolmuşsa cihazın içeriğinin silinmesine yardımcı olur.
- Kimlik ve şifre koruma
  - 2 Adımlı Doğrulama, Güvenlik Anahtarı Olarak Telefon ve Şifre Yöneticisi, Google hesabınızı dışarıdan erişime karşı korur.
  - Güvenlik Kontrolü ve isteğe bağlı Gelişmiş Koruma, cihazın güvenli ve sorunsuz şekilde çalışmasını sağlar.
- Kimlik avına karşı koruma
  - Google Telefon ve Google'dan Mesajlar, dolandırıcılık ve kimlik avı saldırılarını tespit etmeye yardımcı olur.
  - Google Güvenli Tarama küresel olarak 5 milyardan fazla cihazı korur.

Uygulama Güvenliği

Kullanıma hazır kötü amaçlı yazılımdan koruma, kötü uygulamaları devre dışı bırakır ve veri güvenliği bilgileri, uygulama indirirken kullanıcılara şeffaflık sağlar.

- Google Play Store: Makine öğrenimine dayalı saptama araçları ve insan analistler, indirilmek için kullanıcılara sunulmadan önce tüm uygulamaları gözden geçirir. Veri Güvenliği bölümü, uygulamaların ne tür verileri topladığını ve bu verilerin hangi amaçlarla kullanıldığını açıklar.
- Google Play Protect: Her gün 125 milyardan fazla uygulamayı tarar ve güvenlik risklerinin tespit edilmesi durumunda bildirimde bulunur, riskleri ortadan kaldırır ya da etkisiz hâle getirir.
- Uygulama Savunma Birliği (ADA): Google, istihbarat paylaşımı ve koordineli tespit aracılığıyla Android kullanıcılarını Potansiyel Olarak Zararlı Uygulamalardan (PHA'lar) koruyan Uygulama Savunma Birliğini hayata geçirmek için üst düzey mobil tehdit saptama iş ortaklarıyla birlikte çalıştı.

IoT Güvenliği

IoT güvenlik etiketleri, hangi verilerin toplandığı gibi, gizlilik ve güvenlik uygulamalarını bir cihaz üzerinde açık bir şekilde iletir.

- IoT güvenlik etiketleme programları ile ilgili olarak beş temel ilkeye inanıyoruz: Canlı etiket, değerlendirme programları; esneklik, geniş tabanlı şeffaflık ve benimseme teşvikleri ile birlikte güvenlik temel hatları.
- Mevcut ve gelecekteki düzenleyici gereklilikleri için sektör genelinde bir sertifikasyon programını standartlaştırmak amacıyla Bağlanırlık Standartları Birliği (CSA) ve GSM Birliği (GSMA) ile birlikte çalışıyoruz.

İlkelerimiz

Google olarak, bağlı cihazlarımızın güvenliğini ve şeffaflığını geliştirmek için 3 temel ilkeyi uyguluyoruz:

Derinlemesine Savunma: Sorunsuzca ve etkili bir şekilde işleyen, güçlü bir savunma oluşturmak için birlikte çalışan birden fazla güvenlik mimarisi katmanını kullanıyoruz.

Açık ve Şeffaf: TŞeffaflık, felsefemiz açısından büyük öneme sahiptir. Platformlarımızdaki kullanıcıları sürekli olarak bilgilendirerek ve korumamızı artırmak için bilgi paylaşarak açık kaynak bir ekosistemin kapalı bir sistemden daha güvenli olabileceğine inanıyoruz.

Google'ın ve Ekosistemimizin en iyileri: Milyarlarca kullanıcıyı güvende tutmak için Google ve sektör genelinde uzman ekiplerle ortak çalışıyoruz.

Uygulamalar

IoT güvenlik etiketleri: Kontrolü tüketicilere veriyoruz

IoT güvenlik etiketlemesi olmaksızın cihaz üreticilerinin takip edeceği küresel standartlar yoktur. Kullanıcılar, cihazlarının verilerini koruyup korumadığı hakkında hak ettikleri görünürlüğe de sahip değiller. Sektör, IoT güvenliğinin geliştirilmesi ve kontrolün tekrar tüketicilere verilmesi için bir araya gelmelidir. Süreçlerimiz ve ortaklıklarımız aracılığıyla bir IoT güvenlik etiketleme programına doğru çalışıyoruz.

Öncelikle muhtemel güvenlik açıklarını tam olarak saptamak amacıyla haricî güvenlik araştırmalarına yatırım yaparız (Google Nest, Google güvenlik açığı ödül programına katılıyor ve güvenlik açıklarını tespit eden, Google dışından güvenlik araştırmacılarına ödüller sağlıyor).

Bundan sonra, lansmanı takiben en az beş yıl boyunca kritik hata yamaları ve düzeltmeler sağlarız.

2019'da ve sonrasında geliştirilen tüm cihazlarımız, doğru yazılımın çalıştığından ve erişimin korunduğundan emin olmak için Doğrulanmış Başlatma'yı kullanır. Örneğin, Google Nest cihazlarımız, ETSI ve ISO tarafından geliştirilmiş olanlar gibi, sektörce tanınan üçüncü taraf güvenlik standartları kullanılarak doğrulanır.

Bu standartlar ve güvenli Yazılım Geliştirme Yaşam Döngümüz (SDLC), tüketicilerin kötü güvenlik uygulamalarına maruz kalma olasılığını azaltır ve açık ve daha güvenli bir internetin yolunu açar.

Sektör Yatırımlarımız ve Önemli Adımlarımız

2007 Tehlikeli web sitelerini ziyaret ettiklerinde kullanıcıları proaktif şekilde uyarmak için Güvenli Tarama geliştirildi ve bugün 5 milyardan fazla cihazı koruyor.

2010 Devletler ve kurumsal politikaların gizliliği, güvenliği ve çevrimiçi bilgilere erişimi nasıl etkilediğini göstermek için Google Şeffaflık Raporunun lansmanı yapıldı. 2018 yılında Android'e özel olan bir Şeffaflık Raporu ekledik.

2017 Günde 3 milyarı aşkın cihazda 125 milyardan fazla uygulamayı tarayan, bugün en yaygın şekilde kullanılan kötü amaçlı yazılımdan koruma çözümü olan Google Play Protect'in lansmanı yapıldı.

2019 Güvenlik Anahtarı uygulaması Android'de yerleşik bir özellik olarak geliştirildi ve daha sonra 2020 yılında iPhone için kullanıma sunuldu.

2022 Google Play, uygulamaların kullanıcıların verilerini nasıl kullandığı, paylaştığı ve koruduğu hakkında insanlara daha fazla bilgi vermek için bir Veri güvenliği bölümünü hizmete koydu ve Uygulama Savunma Birliği aracılığıyla bağımsız bir güvenlik incelemesi gerçekleştiren herhangi bir uygulama için ilk rozet sistemi hayata geçirildi.

2023 Geçiş anahtarı: şifresiz gelecek, açık standartların FIDO Birliği ve dünya genelindeki teknoloji liderlerine on yıl boyunca teşvik edilmesinin ardından genişletilmiş geçiş anahtarı desteği birlikte kullanıma sunuldu.

Yaklaşımımız

Amacımız açık ve güvenli bir dijital dünya sağlamak

Daha fazla sayıdaki cihazda daha fazla veriyle güvenlik endişeleri ister istemez daha da artacak. Ürün geliştirmemiz, şeffaflık kriterimiz ve sektördeki iş ortaklıklarımız aracılığıyla bağlı cihaz güvenliğinin geleceğini geliştirmeye yardımcı oluyoruz.

Ürün stratejimizin temel taşı, ürünlerimizin varsayılan olarak güvenli olmalarını sağlamaktır. Güvenli Tarama, Google Play Protect ve yerleşik Güvenlik Anahtarları, ürünlerimizde en yüksek seviyede güvenliği sağlamak için mobil cihazları ve uygulamaları korur.

Sorunları nasıl ele aldığımız konusunda açık ve şeffaf olarak ve bağlı cihaz güvenlik bilgilerini paylaşarak güvenlik operasyonlarının yaygınlaştırılmasına yardımcı oluyoruz. Katmanlı güvenlik yaklaşımımızla açık kaynak bir ekosistemin kapalı bir ekosistemden daha güvenli olabileceğine inanıyoruz.

CSA, ADA ve GSMA ile iş birliği yaparak herkes için daha güvenli bir internet ve gelecek amacıyla siber güvenlikte en son teknolojiyi geliştirmek için çalışıyoruz.

Bağlı cihaz güvenliğinin çıtasını yükseltmekte ve herkes için her yerde daha güvenli bir çevrimiçi ortam standardı belirlemekte kararlıyız. Google'ın bağlı cihaz güvenliği alanında kaydettiği ilerleme hakkında daha fazla bilgi edinin: g.co/connecteddevicesafety

Kaynaklar: [1] CNBC Siber Rapor, 9 Ocak 2023, [2] IoT Saldırısı Nedir? IoT Güvenliği Hakkında Ayrıntılı Bilgi, 20 Temmuz 2021