Segurança para dispositivos móveis, aplicativos e IoT

Protegendo dados e dispositivos no mundo todo

Com o aumento de ataques cibernéticos patrocinados por agentes online mal-intencionados, acreditamos que nossos produtos e serviços só podem ser úteis se forem seguros. No Google, estamos mais focados do que nunca em proteger pessoas, organizações e governos compartilhando nossa experiência; capacitar a sociedade para lidar com o dinamismo dos riscos cibernéticos; e criar mecanismos de segurança cibernética cada vez mais sofisticados e um mundo mais seguro para todos.

É crucial estar à frente e ampliar constantemente as soluções de segurança para enfrentar as crescentes ameaças (principalmente quando se trata de proteger dispositivos e aplicativos conectados) a fim de fornecer aos usuários um ambiente seguro, com liberdade de escolha em cada dispositivo.

Desafio

A conectividade tem um preço

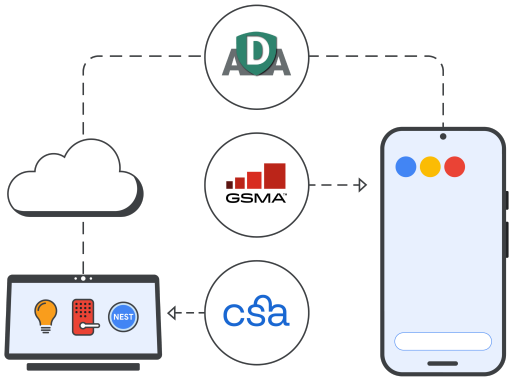
Smartphones, aplicativos e dispositivos IoT fazem parte do nosso cotidiano, e passamos cada vez mais tempo online compartilhando dados valiosos, como informações bancárias e de saúde. Por isso, mais do que nunca, criminosos cibernéticos experientes buscam informações confidenciais nesses dispositivos.

Mais dispositivos, mais dados, mais ameaças

Hoje, existem cerca de 17 bilhões de dispositivos IoT no mundo – de impressoras a controles de portões – repletos de softwares (alguns de código aberto) que podem ser facilmente hackeados.[1] No geral, o número de dispositivos IoT comprometidos praticamente dobrou em 2020.[2]

- Apesar de estarmos cada vez mais conectados por meio de dispositivos IoT, não há padrões globais para medir a segurança desses produtos, ou seja, os consumidores tomam decisões sem terem as informações necessárias.
- Os usuários precisam ter direito à transparência sobre seus produtos digitais, assim como têm o direito de saber a lista de ingredientes dos alimentos ou produtos de limpeza que compram.
- Os dispositivos móveis são apenas um vetor para outras superfícies de ataque, e a interconectividade aumenta a necessidade de transparência em grande escala. A segurança do ecossistema de dispositivos conectados é tão importante quanto a segurança de redes e sistemas.

Colaboração com organizações do setor



Nossa solução

No Google, estamos aprimorando a segurança e a transparência de dispositivos conectados através da segurança de dispositivos móveis, aplicativos e IoT:

Segurança para dispositivos móveis

O Android, nosso sistema operacional de código aberto, tem uma abordagem de segurança em camadas para aumentar a proteção de dispositivos móveis:

- Segurança em camadas
  - Inicialização verificada e proteção contra reversão e redefinição de fábrica garantem a versão mais recente e segura do Android.
  - PIN e autenticação biométrica protegem contra acesso externo.
  - O recurso “Encontre Meu Dispositivo” ajuda a localizar ou limpar o aparelho case ele seja roubado ou perdido.
- Proteção de identidade e senha
  - A verificação em duas etapas, o telefone como chave de segurança e o Gerenciador de senhas protegem sua conta do Google contra acesso externo.
  - A verificação de segurança e a proteção avançada opcional mantêm o dispositivo funcionando com segurança e eficiência.
- Proteção antiphishing
  - Os apps Phone by Google e Messages by Google ajudam a detectar e prevenir golpes e ataques de phishing.
  - A Navegação Segura do Google protege mais de 5 bilhões de dispositivos em todo o mundo.

Segurança para aplicativos

O antimalware de fábrica ajuda a bloquear aplicativos nocivos, e as informações de segurança de dados fornecem transparência na hora de baixar aplicativos.

- Loja Google Play: Detectores alimentados por aprendizado de máquina e analistas humanos revisam todos os aplicativos antes de disponibilizá-los para download. A seção “Segurança de dados” explica quais tipos de dados são coletados pelos aplicativos e como eles são usados.
- Google Play Protect: Verifica mais de 125 bilhões de aplicativos todos os dias e os notifica, remove ou desativa em caso de riscos à segurança.
- App Defense Alliance (ADA): O Google se uniu a grandes nomes da detecção de ameaças móveis para lançar a App Defense Alliance. Ela ajuda a proteger os usuários do Android contra aplicativos potencialmente nocivos (PHAs) usando inteligência compartilhada e detecção coordenada.

Segurança para IoT

Os rótulos de segurança para IoT transmitem claramente as práticas de privacidade e segurança de um dispositivo, como os dados que são coletados.

- Acreditamos em cinco princípios básicos para esquemas de rotulagem de segurança da IoT: rótulo ativo, esquemas de avaliação, segurança padronizada e flexível, transparência ampla e incentivos de uso.
- Estamos trabalhando com a Connectivity Standards Alliance (CSA) e a GSM Alliance (GSMA) para padronizar um programa de certificação para todo o setor que abranja regulamentos atuais e futuros.

Nossos princípios

No Google, aplicamos três princípios fundamentais para aumentar a segurança e a transparência dos nossos dispositivos conectados:

Defesa abrangente: Utilizamos uma arquitetura de segurança em várias camadas. Elas funcionam juntas para criar uma defesa potente, que funciona com leveza e eficiência.

Abertura e transparência: A transparência é crucial na nossa filosofia. Ao manter nossos usuários informados e compartilhar conhecimento para reforçar a proteção, acreditamos que o ecossistema de código aberto pode ser mais seguro do que o fechado.

O melhor do Google e do nosso ecossistema: Trabalhamos com equipes de especialistas do Google e do setor para ajudar a manter bilhões de usuários seguros.

Aplicações

Rótulos de segurança para IoT: o controle nas mãos dos consumidores

Sem uma rotulagem de segurança da IoT, não há padrões globais a serem seguidos pelos fabricantes de dispositivos. Injustamente, os usuários também ficam sem saber se os dispositivos protegem seus dados. O setor precisa se unir para impulsionar a segurança da IoT e devolver o controle aos consumidores. Estamos trabalhando na rotulagem de segurança para IoT com ajuda de nossos processos e parcerias.

Primeiro, investimos em pesquisa de segurança externa para detectar possíveis vulnerabilidades (o Google Nest é parte do programa de recompensa de vulnerabilidade do Google, oferecendo incentivos a pesquisadores externos que detectam vulnerabilidades).

A partir daí, emitimos patches e correções de bugs críticos por pelo menos cinco anos após o lançamento.

Todos os nossos dispositivos desenvolvidos a partir de 2019 usam a Inicialização verificada para garantir a execução do software correto e a proteção do acesso. Por exemplo, os dispositivos Google Nest são validados usando padrões de segurança reconhecidos pelo setor, como os desenvolvidos pelo ETSI e ISO.

Esses padrões e o ciclo do desenvolvimento de software seguro (SDLC) reduzem a probabilidade de exposição a práticas de segurança inadequadas, abrindo caminho para uma internet mais aberta e segura.

Investimentos e marcos

2007 — **Estabelecimento do Navegação segura** que alerta quando os usuários visitam sites perigosos e, hoje, protege mais de 5 bilhões de dispositivos.

2010 — **Lançamento do Relatório de Transparência do Google** mostrando como governos, políticas e ações corporativas afetam a privacidade, a segurança e o acesso a informações online. Em 2018, adicionamos um Relatório de Transparência específico para Android.

2017 — **Lançamento do Google Play Protect** que hoje é a solução antimalware mais usada, verificando mais de 125 bilhões de aplicativos por dia em mais de 3 bilhões de dispositivos.

2019 — **Incorporação da chave de segurança** ao Android e, em 2020, ao iPhone.

2022 — **O Google Play lança** uma seção de segurança de dados para oferecer mais informações sobre como os aplicativos coletam, compartilham e protegem os dados dos usuários, além do primeiro sistema para rotular aplicativos que fazem uma análise de segurança independente com a App Defense Alliance.

2023 — **Senhas de acesso: o futuro do login sem senha** está sendo colocado em prática, ampliando o suporte a senhas de acesso após uma década definindo padrões globais com a FIDO Alliance e líderes tecnológicos do mundo todo.

Nossa abordagem

Compromisso com um mundo digital aberto e seguro

Com mais dados em mais dispositivos e em diferentes redes, as preocupações com a segurança só vão aumentar. Estamos ajudando a desenvolver o futuro da segurança de dispositivos conectados criando produtos, critérios de transparência e parcerias no setor

Um dos pilares da nossa estratégia é criar produtos seguros por padrão. Navegação segura, Google Play Protect e chaves de segurança integradas protegem dispositivos móveis e aplicativos, oferecendo o mais alto nível de segurança em nossos produtos.

Ajudamos a democratizar a segurança sendo abertos e transparentes sobre como lidamos com problemas e compartilhando conhecimento sobre segurança de dispositivos conectados. Acreditamos que, com a segurança em camadas, o ecossistema de código aberto pode ser mais seguro do que o fechado.

Ao colaborar com a CSA, ADA e GSMA, nos esforçamos para promover uma segurança cibernética sofisticada, com uma internet e um futuro mais seguros para todos.

Estamos comprometidos em elevar a segurança de dispositivos conectados e definir o padrão para um ambiente online mais seguro – para todo mundo, em todos os lugares. Saiba mais sobre os avanços do Google na segurança de dispositivos conectados: g.co/connecteddevicesafety

Fontes: [1] CNBC Cyber Report, 9 de janeiro de 2023, [2] What is an IoT Attack? The Ins and Outs of IoT Security, J20 de julho de 2021