Relatório interno do NIST NIST IR 8425 por

Perfil da linha de base principal de IoT para produtos de IoT para consumidores

Michael Fagan
Katerina Megas
Paul Watrobski
Jeffery Marron
Barbara Cuthill

Esta publicação está disponível gratuitamente no site:
https://doi.org/10.6028/NIST.IR.8425.por

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Relatório interno do NIST
NIST IR 8425 por

Perfil da linha de base principal de IoT para produtos de IoT para consumidores

Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
Divisão de Segurança Cibernética Aplicada
Laboratório de Tecnologia da Informação

Esta publicação está disponível gratuitamente no site:
https://doi.org/10.6028/NIST.IR.8425.por

setembro 2022

Departamento de Comércio dos EUA
Gina M. Raimondo, Secretária

Instituto Nacional de Padrões e Tecnologia
Laurie E. Locascio, Diretora do NIST e Subsecretária de Comércio para Padrões e Tecnologia

Determinadas entidades comerciais, equipamentos ou materiais podem ser identificados neste documento para descrever adequadamente um procedimento ou conceito experimental. Essa identificação não tem a intenção de implicar recomendação ou endosso do Instituto Nacional de Padrões e Tecnologia (NIST), nem que as entidades, os materiais ou os equipamentos sejam necessariamente os melhores disponíveis para a finalidade.

Pode haver referências nesta publicação a outras publicações atualmente em desenvolvimento pelo NIST, de acordo com suas responsabilidades legais atribuídas. As informações contidas nesta publicação, incluindo conceitos e metodologias, podem ser usadas por órgãos federais mesmo antes da conclusão dessas publicações complementares. Assim, até que cada publicação seja concluída, os requisitos, diretrizes e procedimentos atuais, quando existentes, permanecem em vigor. Para fins de planejamento e transição, os órgãos federais podem querer acompanhar de perto o desenvolvimento dessas novas publicações do NIST.

As organizações são incentivadas a revisar todos os rascunhos de publicações durante os períodos de comentários públicos e fornecer feedback ao NIST. Muitas publicações sobre segurança cibernética do NIST, além das mencionadas acima, estão disponíveis em https://csrc.nist.gov/publications.

Políticas da Série Técnica do NIST
Declarações de direitos autorais, uso justo e licenciamento
Sintaxe do identificador de publicação da série técnica do NIST

Histórico de Publicações
Aprovado pelo Conselho de Revisão Editorial do NIST em 2022-09-08

Como citar esta publicação da série técnica do NIST:
Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B (2022) Perfil da Linha de Base Principal de IoT para Produtos de IoT para Consumidores. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Relatório Interagencial ou Interno do NIST (IR) NIST IR 8425. https://doi.org/10.6028/NIST.IR.8425

Autor ORCID iDs
Michael Fagan: 0000-0002-1861-2609
Katerina N. Megas: 0000-0002-2815-5448
Paul Watrobski: 0000-0002-6449-3030
Jeffrey Marron: 0000-0002-7871-683X
Barbara B. Cuthill: 0000-0002-2588-6165

Informações de contato
iotsecurity@nist.gov

Instituto Nacional de Padrões e Tecnologia
Aos cuidados de: Divisão de Segurança Cibernética Aplicada, Laboratório de Tecnologia da Informação
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Todos os comentários estão sujeitos à divulgação de acordo com a Lei de acesso à informação dos Estados Unidos (FOIA).

A versão oficial em inglês desta publicação está disponível gratuitamente no National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.IR.8425.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.IR.8425.

Relatórios sobre tecnologia de sistemas de computador

O ITL (Information Technology Laboratory, Laboratório de Tecnologia da Informação) do NIST (National Institute of Standards and Technology, Instituto Nacional de Padrões e Tecnologia) promove a economia e o bem-estar público dos EUA, fornecendo liderança técnica para a infraestrutura de medição e padrões do país. O ITL desenvolve testes, métodos de teste, dados de referência, implementações de prova de conceito e análises técnicas para promover o desenvolvimento e o uso produtivo da tecnologia da informação. As responsabilidades do ITL incluem o desenvolvimento de padrões e diretrizes gerenciais, administrativos, técnicos e físicos para a segurança econômica e a privacidade de informações não relacionadas à segurança nacional em sistemas de informações federais.

Resumo

Esta publicação documenta o perfil do consumidor da linha de base principal da Internet das Coisas (IoT) do NIST e identifica os recursos de segurança cibernética normalmente necessários para o setor de IoT do consumidor (ou seja, produtos de IoT para uso doméstico ou pessoal). Ela também pode ser um ponto de partida para as empresas considerarem a compra de produtos de IoT. O perfil do consumidor foi desenvolvido como parte da resposta do NIST à Ordem Executiva 14028 e foi publicado inicialmente em *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (Critérios recomendados para rotulagem de segurança cibernética para produtos de Internet das Coisas (IoT) para consumidores)*. Os recursos do perfil do consumidor são formulados como resultados de segurança cibernética que devem ser aplicados a todo o produto de IoT. Este documento também discute os fundamentos para o desenvolvimento do perfil de consumidor recomendado e considerações relacionadas. O NIST analisou um conjunto de documentos relevantes para informar o perfil do consumidor e se envolveu com as partes interessadas em um esforço de um ano para desenvolver as recomendações.

Palavras-Chave

Internet das Coisas (IoT); IoT do consumidor; segurança cibernética; produtos de IoT; privacidade; segurança; produtos seguros.

Público

O público-alvo deste relatório são os fabricantes de produtos de consumo, especialmente os responsáveis pela segurança dos produtos, os varejistas, os integradores relacionados e as empresas de suporte técnico que atendem aos setores de consumo e de negócios, bem como os órgãos de teste e certificação interessados em estabelecer linhas de base dos recursos de segurança cibernética de IoT.

Aviso de Divulgação de Patente

AVISO: O ITL solicitou que os detentores de reivindicações de patentes cujo uso possa ser necessário para a conformidade com as orientações ou requisitos desta publicação divulguem tais reivindicações de patentes ao ITL. No entanto, os detentores de patentes não são obrigados a responder às solicitações de patentes do ITL e o ITL não realizou uma pesquisa de patentes para identificar quais patentes, se houver, podem se aplicar a esta publicação.

Até a data da publicação e após a(s) solicitação(ões) para a identificação de reivindicações de patentes cujo uso pode ser necessário para a conformidade com as orientações ou requisitos desta publicação, nenhuma reivindicação de patente foi identificada para o ITL.

O ITL não faz nenhuma declaração nem deixa implícito que as licenças não são necessárias para evitar a violação de patentes no uso desta publicação.

Índice

Lista de tabelas

Lista de figuras

Agradecimentos

Os autores gostariam de agradecer a todos os colaboradores desta publicação, incluindo os participantes de workshops e outras sessões interativas; os indivíduos e organizações dos setores público e privado, incluindo fabricantes de vários setores, bem como várias organizações comerciais de fabricantes, que forneceram feedback durante o período de resposta da Ordem Executiva 14028 do NIST. Agradecimentos especiais aos membros da equipe de segurança cibernética para IoT, Rebecca Herold, Brad Hoehn e David Lemire.

1. Introdução

Em 12 de maio de 2021, o presidente emitiu a Ordem Executiva (EO) 14028, que, entre outras diretrizes, solicitava que o NIST recomendasse requisitos para um programa de rotulagem de segurança cibernética de produtos de IoT para consumidores. Como parte da resposta do NIST a essa diretriz[1], foi criado um perfil da linha de base principal de IoT[2] para produtos de IoT para consumidores. Esse perfil serviu como parte das recomendações que o NIST publicou em resposta à EO em fevereiro de 2022, intitulado *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (Critérios recomendados para rotulagem de segurança cibernética para produtos de Internet das Coisas (IoT) para consumidores)* [EO_Critérios].

O perfil se baseia na série NISTIR 8259, ampliando a linha de base principal de IoT para produtos de IoT para consumidores. O NISTIR 8259, *Atividades fundamentais de segurança cibernética para fabricantes de dispositivos de IoT* [IR8259], fornece orientação fundamental para os fabricantes de dispositivos de IoT referentes ao desenvolvimento de dispositivos de IoT que podem ser usados com segurança pelos clientes. A NISTIR 8259 não se destina a nenhum setor específico de IoT, mas discute como os fabricantes podem abordar a segurança cibernética para dispositivos de IoT em geral. A NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline (Linha de Base Principal do Recurso de Segurança Cibernética de Dispositivos IoT)* [IR8259A] e a NISTIR 8295B, *IoT Non-Technical Supporting Capability Core Baseline (Linha de Base Principal de Recursos de Suporte Não Técnicos de IoT)* [IR259B] definem a linha de base principal do recurso de segurança cibernética do dispositivo de IoT (também chamada de linha de base principal). A linha de base principal é um ponto de partida para os fabricantes usarem na identificação dos recursos de segurança cibernética que seus clientes podem esperar dos dispositivos de IoT que eles criam. A NISTIR 8259A discute os recursos de segurança cibernética do dispositivo, que são funções ou recursos implementados pelo dispositivo por meio de seu próprio hardware e software. Por exemplo, a NISTIR 8259A discute conceitos como proteção de dados, controle de acesso e atualização de software, entre outros. A NISTIR 8259B discute os recursos de suporte não técnicos, que são ações tomadas pelas organizações para apoiar a segurança cibernética do dispositivo. Por exemplo, a NISTIR 8259B discute conceitos como educação e conscientização e recebimento de informações e consultas (por exemplo, por fabricantes/desenvolvedores).

Assim como a NISTIR 8259, esses documentos de linha de base não são específicos do setor ou do caso de uso e, em vez disso, apresentam um ponto de partida para *qualquer* dispositivo de IoT. A adaptação dos recursos de linha de base para um setor e/ou caso de uso específico requer uma forma de criação de perfil. O processo de criação de perfil usando a série NISTIR 8259 orienta o criador de perfil a coletar informações específicas do setor/caso de uso e interpretar os impactos relevantes para selecionar os recursos de linha de base mais aplicáveis às necessidades e à meta dos clientes no setor/caso de uso.

[1] Para obter mais informações sobre a resposta do NIST à solicitação de recomendações da EO 14028 para um rótulo de segurança cibernética de produtos de IoT para consumidores, acessar https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0

[2] Os termos *linha de base principal, linha de base principal de IoT e linha de base principal dos recursos do dispositivo de IoT* referem-se ao conjunto de recursos apresentados nos NISTIRs 8259A e 8259B.

O restante deste documento descreve os resultados desse processo de criação de perfil para o setor de consumo e está organizado da seguinte forma:

- A Seção 2 explica a aplicabilidade pretendida do perfil do consumidor aos produtos de IoT do consumidor e define o perfil do consumidor.
- A Seção 3 descreve mais detalhadamente o processo usado para desenvolver o perfil do consumidor.
- A Seção 4 explora considerações adicionais que os leitores devem fazer ao usar o perfil do consumidor.

2. Perfil do Consumidor da Linha de Base Principal de IoT

Esta seção se baseia no whitepaper *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (Critérios recomendados para rotulagem de segurança cibernética para produtos de Internet das Coisas (IoT) para consumidores)* [EO_Critérios]. Primeiro, é definido o escopo de um "produto de IoT" e, em seguida, é apresentado o perfil do produto de IoT do consumidor da linha de base principal de IoT.

2.1. Declaração do Escopo do Produto de IoT

Produtos de IoT geralmente constituem um conjunto de componentes de sistema que trabalham juntos para oferecer funcionalidade realizada no ponto final ou no componente "dispositivo" do produto. O NIST descreve um dispositivo de IoT como um equipamento de computação com pelo menos um transdutor (ou seja, sensor ou atuador) e pelo menos uma interface de rede [IR8259]. Todos os produtos de IoT contêm pelo menos um dispositivo de IoT e podem conter apenas esse componente do produto. Em muitos casos, o produto de IoT pode ser adquirido como uma peça de equipamento (ou seja, o dispositivo de IoT), mas ainda requer outros componentes para funcionar, como um backend (por exemplo, servidor em nuvem) ou um aplicativo de usuário complementar em um computador pessoal ou smartphone.

Os produtos complexos de IoT podem conter vários dispositivos físicos de IoT, conter outros tipos de equipamentos ou se conectar a vários backends ou aplicativos complementares como componentes. Embora haja possivelmente muitas combinações de componentes que podem criar um produto de IoT, é útil pensar em três tipos específicos de componentes de produtos de IoT (além do próprio dispositivo de IoT, que está sempre presente em um produto de IoT):

- Hardware especializado de rede/gateway (por exemplo, um hub no sistema em que o dispositivo de IoT é usado).
- Software de aplicativo complementar (por exemplo, um aplicativo móvel para comunicação com o dispositivo de IoT).
- Backends (por exemplo, um serviço de nuvem ou vários serviços que podem armazenar e/ou processar dados do dispositivo de IoT).

Alguns componentes do produto de IoT, como o(s) dispositivo(s) de IoT (e talvez um hardware especializado de rede/gateway[3]), estarão "na caixa" que o cliente compra.[4] Outros componentes, como software de aplicativo complementar ou back-ends, existirão "fora da caixa[5]", mas, ainda assim, fazem parte do produto de IoT por meio do suporte que fornecem para a operação do produto de IoT. Independentemente dessas relações, esses componentes adicionais do produto têm acesso ao dispositivo de IoT e aos dados que ele cria e usa, o que os torna possíveis vetores de ataque que podem afetar o dispositivo de IoT, o cliente e outros (por exemplo, por meio de ataques a sistemas, redes locais ou à Internet em geral). Como esses componentes adicionais podem introduzir riscos novos ou exclusivos ao produto de IoT, todo o produto de IoT, inclusive os componentes auxiliares, deve ser protegido.

Nota Sobre Considerações de Avaliação de Conformidade de Componentes de IoT

Este documento discute os recursos no nível do produto de IoT, mas os produtos de IoT são definidos como um conjunto de componentes de produtos de IoT. Ao considerar o processo de avaliação da conformidade nesse contexto, é importante observar as complexidades da avaliação da ampla variedade de combinações de componentes de IoT que poderiam criar um produto. Além disso, alguns desses componentes de produtos de IoT podem ser total ou parcialmente *modularizados*, em que os clientes podem escolher o componente e/ou a plataforma do componente. Por exemplo, alguns softwares de aplicativos complementares serão executados em sistemas operacionais móveis ou por meio de um navegador da Web, para os quais a segurança cibernética vai muito além da função que o componente pode desempenhar no produto de IoT. Nesses casos, a avaliação desses componentes de produtos de IoT quanto à conformidade com os recursos de segurança cibernética no perfil do consumidor deve considerar esse fato e utilizar os padrões e/ou mecanismos de conformidade existentes como parte do mecanismo de conformidade do produto da IoT, tanto quanto possível. Por exemplo, podem existir programas de certificação de segurança cibernética de sistemas operacionais ou de nuvem que demonstrem suporte parcial aos recursos de segurança cibernética identificados no perfil do consumidor, mas, em muitos casos, o suporte que o componente de IoT oferece ao produto será obtido com o uso de software e/ou hardware de aplicativos

[3] Alguns hardwares especiais de rede/gateway podem ser adquiridos pelo cliente separadamente, mas são necessários para que o produto de IoT funcione além dos recursos básicos. Na maioria dos casos em que um produto de IoT requer hardware de rede/gateway especializado adquirido separadamente, esse hardware executará tarefas específicas e consistentes na implementação de um produto de IoT (por exemplo, tradução de protocolo). Por exemplo, alguns produtos de IoT exigem conexões de rede que não sejam Wi-Fi/ethernet convencionais, como Bluetooth, Zigbee ou Z-Wave, que precisariam de um *hub* ou *gateway* para permitir uma conectividade mais ampla (ou seja, além de Wi-Fi e/ou ethernet). Esse *hub* ou *gateway* nem sempre pode ser incluído como parte de um produto de IoT, mas, em vez disso, pode ser considerado parte da infraestrutura de rede do cliente, da mesma forma que um roteador Wi-Fi pode ser considerado para produtos de IoT que usam Wi-Fi.

[4] Os componentes "na caixa", especialmente o(s) dispositivo(s) de IoT que serve(m) como ponto final do produto, podem ser considerados a *face* do produto de IoT, pois é com eles que o cliente irá lidar, gerenciar e usar fisicamente. Embora outros componentes possam ser vitais para a operação do produto de IoT (incluindo a segurança cibernética), o(s) dispositivo(s) de IoT desempenha(m) um papel central no produto de IoT e, em geral, é o foco da operação do produto de IoT.

[5] Alguns componentes "fora da caixa" podem ser totalmente remotos em relação ao cliente, enquanto outros podem estar fisicamente presentes no ambiente do cliente (por exemplo, dentro de sua casa), mas, ainda assim, separados do(s) dispositivo(s) de IoT.

adicionais que podem não ser considerados ou avaliados pelos programas existentes. A avaliação da segurança cibernética do produto de IoT pode, portanto, aceitar a certificação existente e avaliar a segurança cibernética do software/hardware do aplicativo adicional.

Nesse contexto, um produto de IoT é definido como um dispositivo de IoT ou dispositivos de IoT e quaisquer componentes adicionais do produto que sejam necessários para usar o dispositivo de IoT além dos recursos operacionais básicos. Por exemplo, uma lâmpada inteligente não conectada ainda pode iluminar em uma cor, mas seus recursos inteligentes, como mudanças de cor, não podem ser usados sem outros componentes do produto.

2.2. Perfil do Consumidor

Esta seção define os recursos de segurança cibernética[6] esperados dos produtos de IoT e dos desenvolvedores de produtos de IoT como parte de um perfil de consumidor.

Recomenda-se que os critérios do produto sejam aplicados ao produto de IoT como um todo, bem como a cada componente individual do produto de IoT, conforme apropriado. A maioria dos critérios diz respeito diretamente ao produto de IoT e espera-se que sejam atendidos por meios de software e/ou hardware implementados no produto de IoT. Alguns critérios se aplicam ao desenvolvedor do produto de IoT, e não diretamente ao produto de IoT. Espera-se que esses critérios sejam atendidos por meio de ações e apoiados por afirmações e evidências do desenvolvedor, e não do próprio produto de IoT.

A figura a seguir apresenta os recursos de alto nível dos produtos de IoT e as atividades do desenvolvedor de produtos de IoT[7] desenvolvidas com base nas NISTIRs 8259A e 8259B, respectivamente, que são discutidas nas seções a seguir.

[6] O termo recurso é geralmente usado neste documento para seguir a série NISTIR 8259, mas esses mesmos recursos foram apresentados como "resultados" na Seção 2.2 dos *Critérios Recomendados para Rotulagem de Segurança Cibernética para Produtos de Internet das Coisas (IoT) para Consumidores*. Esses termos são sinônimos e podem ser usados de forma intercambiável no contexto deste documento e do whitepaper.
[7] Na série NISTIR 8259, os fabricantes de dispositivos de IoT são mencionados e podem ser a mesma entidade que um desenvolvedor de produtos de IoT discutido aqui. A natureza multicomponente dos produtos de IoT, no entanto, aumenta a chance de que a entidade que leva um produto de IoT ao mercado não tenha fabricado o(s) dispositivo(s) físico(s) de IoT, mas sim usado dispositivos fabricados por outra entidade para criar um produto de IoT. Portanto, o termo desenvolvedor de produtos de IoT é usado neste documento.

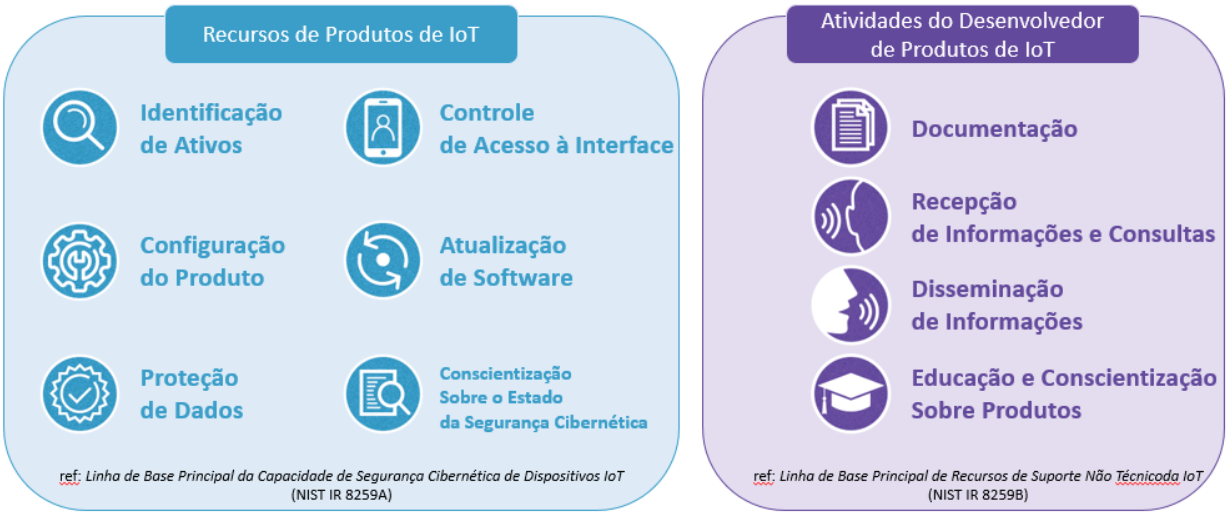

Fig. 1. Recursos Identificados para o Perfil do Consumidor.

O nome de cada recurso e a definição de alto nível do recurso são apresentados, seguidos de uma lista alfanumérica de subcritérios para cada recurso. Para alguns subcritérios,[8] detalhes adicionais do resultado (ou seja, texto normativo) são listados após o texto **em negrito**, enquanto explicações e exemplos adicionais (ou seja, texto informativo) são listados após o texto *em itálico* . Por fim, cada recurso é acompanhado de uma breve descrição da utilidade pretendida para a segurança cibernética do recurso.

[8] Os subcritérios têm o objetivo de fornecer detalhes adicionais sobre como o resultado descrito na definição de recurso de alto nível pode ser alcançado por um produto de IoT. Os subcritérios podem não abranger todo o suporte possível necessário para um resultado em todos os casos de uso, e os subcritérios também podem não se aplicar a todos os casos de uso.

2.2.1. Recursos de Produtos de IoT

Identificação de Ativos

O produto de IoT é identificável de forma exclusiva e registra todos os componentes de IoT do produto.

1. O produto de IoT pode ser identificado exclusivamente pelo cliente e por outras entidades autorizadas (por exemplo, o desenvolvedor do produto de IoT).[9]
2. O produto de IoT identifica exclusivamente cada componente do produto IoT e mantém um inventário atualizado[10] dos componentes do produto conectado.

Utilitário de segurança cibernética: A capacidade de identificar produtos de IoT e seus componentes é necessária para dar suporte a atividades como gerenciamento de ativos para atualizações, proteção de dados e recursos forenses digitais para resposta a incidentes.

[9] Em alguns casos, pode haver um identificador exclusivo para o próprio produto de IoT (independente até mesmo do identificador do dispositivo de IoT), mas, em muitos casos, a identificação do produto de IoT pode ser interpretada como a identificação de um dos componentes de IoT. Para garantir a exclusividade do identificador do produto em todas as instâncias do produto, normalmente seria o dispositivo de IoT ou algum outro componente "na caixa", em vez de um componente compartilhado por muitas instâncias, como o backend.
[10] Os inventários podem residir em um componente (por exemplo, dispositivo IoT, aplicativo back-end) ou em vários componentes (por exemplo, alguns componentes são inventariados em hardware de rede/gateway especializado), dependendo da arquitetura do produto IoT.

Configuração do Produto

A configuração do produto de IoT pode ser alterada. Há a possibilidade de restaurar uma configuração padrão segura, e toda e qualquer alteração só pode ser realizada por indivíduos, serviços e outros componentes do produto de IoT autorizados.

1. Indivíduos autorizados (ou seja, o cliente), serviços e outros componentes do produto IoT podem alterar as definições de configuração do produto IoT por meio de um ou mais componentes do produto IoT.[11]
2. Indivíduos autorizados (ou seja, o cliente), serviços e outros componentes do produto de IoT podem restaurar o produto de IoT para uma configuração padrão segura (ou seja, não inicializada).
3. O produto de IoT aplica definições de configuração aos componentes de IoT aplicáveis.

Utilitário de segurança cibernética: A capacidade de alterar aspectos de como o produto de IoT funciona pode ajudar os clientes a adaptarem a funcionalidade do produto de IoT às suas necessidades e objetivos. Os clientes podem configurar seus produtos de IoT para evitar ameaças e riscos específicos que conhecem com base em seu apetite de risco.

[11] Para alguns componentes, pode haver configuração relevante para a segurança cibernética de aspectos do componente (por exemplo, plataforma ou infraestrutura de back-ends) que não estão adequadamente no escopo do gerenciamento pelo produto de IoT e/ou cliente. Por exemplo, na maioria dos casos, o software do aplicativo que acompanha o produto de IoT não deve gerenciar a segurança cibernética do sistema operacional em que o software é executado.

Proteção de Dados

O produto de IoT protege os dados armazenados em todos os componentes do produto de IoT e transmitidos entre os componentes do produto de IoT e fora do produto de IoT contra acesso, divulgação e modificação não autorizados.

1. Cada componente de produto de IoT protege os dados que armazena por meios seguros.
2. O produto de IoT tem a capacidade de excluir ou tornar inacessíveis os dados armazenados que são coletados de ou sobre o cliente, a residência, a família etc.
3. Quando os dados são enviados entre os componentes do produto IoT ou fora dele, são usadas proteções para a transmissão de dados.[12]

Utilitário de segurança cibernética: Manter a confidencialidade, a integridade e a disponibilidade dos dados é fundamental para a segurança cibernética dos produtos de IoT. Os clientes esperam que os dados sejam protegidos e que a proteção dos dados ajude a garantir a funcionalidade segura e pretendida do produto de IoT.

[12] Isso pode incluir a capacidade de se comunicar com componentes do produto que não podem implementar o recurso de proteção de dados da mesma forma que outros componentes (por exemplo, não podem oferecer suporte à criptografia adequada). Qualquer comunicação desse tipo (por exemplo, dados transmitidos com proteção inferior ou limitada) ainda deve ser realizada de forma a reduzir o risco subsequente, como um protocolo de transmissão de rede local e/ou de curto alcance (por exemplo, Zigbee, Bluetooth) para se comunicar com alguns componentes do produto em circunstâncias limitadas, mas necessárias.

Controle de Acesso à Interface

O produto de IoT restringe o acesso lógico às interfaces locais e de rede – e aos protocolos e serviços usados por essas interfaces – somente a indivíduos, serviços e componentes autorizados do produto IoT.

1. Cada componente do produto de IoT controla o acesso de e para todas as interfaces (por exemplo, interfaces locais, acessíveis externamente ou não, interfaces de rede, protocolos e serviços) para limitar o acesso somente a entidades autorizadas. **No mínimo, o componente do produto IoT deve:**
    a. Usar e ter acesso somente às interfaces necessárias para a operação do produto de IoT. Todos os outros canais e o acesso aos canais são removidos ou protegidos.
    b. Para todas as interfaces necessárias para o uso do produto de IoT, ter medidas de controle de acesso (por exemplo, autenticação multifatorial baseada em senha exclusiva, portas de interface física inacessíveis do lado de fora de um componente).
    c. Para todas as interfaces, os privilégios de acesso e modificação são limitados.
2. Alguns componentes de produtos de IoT, mas não necessariamente todos, têm os meios para proteger e manter o controle de acesso à interface. **No mínimo, o produto de IoT deve:**
    a. Validar se os dados compartilhados entre os componentes do produto de IoT correspondem às definições especificadas de formato e conteúdo.
    b. Impedir transmissões não autorizadas ou acesso a outros componentes do produto.
    c. Manter o controle de acesso adequado durante a conexão inicial (ou seja, na integração) e ao restabelecer a conectividade após a desconexão ou interrupção.

Utilitário de segurança cibernética: A enumeração e o controle do acesso a todas as interfaces internas e externas do produto de IoT ajudarão a preservar a confidencialidade, a integridade e a disponibilidade do produto de IoT, de seus componentes e dados, ajudando a impedir o acesso e a modificação não autorizados.

Atualização de Software

O software[13] de todos os componentes de produtos de IoT pode ser atualizado por indivíduos, serviços e outros componentes de produtos de IoT autorizados somente por meio de um mecanismo seguro e configurável, conforme apropriado para cada componente de produto da IoT.

1. Cada componente do produto de IoT pode receber, verificar e aplicar atualizações de software verificadas.
2. O produto de IoT implementa medidas para manter o software dos componentes do produto de IoT atualizado (ou seja, aplicação automática de atualizações ou notificação consistente ao cliente sobre as atualizações disponíveis por meio do produto de IoT).

Utilitário de segurança cibernética: O software pode ter vulnerabilidades descobertas depois que o produto de IoT foi implantado; os recursos de atualização de software podem ajudar a garantir a entrega segura de patches de segurança.

[13] Isso inclui código executável, bem como bibliotecas de software, pacotes de suporte e outros dados de software não executáveis.

Conscientização sobre o Estado da Segurança

O produto de IoT oferece suporte à detecção de incidentes de segurança cibernética que afetam ou foram afetados pelos componentes do produto de IoT e pelos dados que eles armazenam e transmitem.

1. O produto de IoT captura e registra com segurança informações sobre o estado dos componentes de IoT[14] que podem ser usadas para detectar incidentes de segurança cibernética que afetam ou foram afetados pelos componentes do produto de IoT e pelos dados que eles armazenam e transmitem.

Utilitário de segurança cibernética: A proteção dos dados e a garantia da funcionalidade adequada podem ser apoiadas pela capacidade de alertar o cliente quando o dispositivo começa a operar de forma inesperada, o que pode significar que está havendo tentativa de acesso não autorizado, carregamento de malware, criação de botnets, erros de software do dispositivo ou outros tipos de ações que não foram iniciadas pelo usuário do produto de IoT ou pretendidas pelo desenvolvedor.

[14] As informações sobre o estado dos componentes de IoT que seriam úteis para detectar incidentes de segurança cibernética são altamente contextuais para o produto da IoT, seus componentes e sua operação. Na maioria dos casos, devem ser capturadas informações temporais, como registro de data e hora ou dados de localização (digitais ou físicos). A versão do software e do hardware e o estado operacional (por exemplo, falhas conhecidas ou exceções lançadas) podem ajudar a detectar vulnerabilidades de segurança cibernética (por exemplo, um software ou hardware específico pode ter vulnerabilidades conhecidas). As informações de estado de segurança cibernética também podem conter registros de comandos e ações recebidos e executados pelo produto de IoT ou outros dados que sejam significativos para o produto de IoT e como ele funciona e, portanto, são úteis para detectar incidentes.

2.2.2. Recursos de Suporte Não Técnico de Produtos de IoT

Documentação

O desenvolvedor de produtos de IoT cria, reúne e armazena[15] informações relevantes para a segurança cibernética do produto de IoT e seus componentes antes da compra pelo cliente e durante todo o desenvolvimento de um produto e seu ciclo de vida subsequente.

1. Durante todo o ciclo de vida do desenvolvimento, o desenvolvedor do produto de IoT cria ou reúne e armazena informações relevantes para a segurança cibernética do produto de IoT e seus componentes, **incluindo**:
    a. Suposições feitas durante o processo de desenvolvimento e outras expectativas relacionadas ao produto de IoT, **incluindo**:
        i. Clientes esperados e casos de uso.
        ii. Uso e características físicas, incluindo a segurança do local do produto de IoT e de seus componentes (por exemplo, uma câmera para uso dentro de casa que tenha um botão de desligamento no dispositivo versus uma câmera de segurança para uso fora de casa que não tenha um botão de desligamento no dispositivo).
        iii. Acesso e requisitos de rede (por exemplo, requisitos de largura de banda).
        iv. Dados criados e manipulados pelo produto de IoT.
        v. Quaisquer entradas e saídas de dados esperadas (incluindo códigos de erro, frequência, tipo/forma, intervalo de valores aceitáveis etc.).
        vi. Os requisitos de segurança cibernética assumidos pelo desenvolvedor do produto de IoT para o produto de IoT.
        vii. Quaisquer leis e regulamentos com os quais o produto IoT e as atividades de suporte relacionadas estejam em conformidade.
        viii. Tempo de vida útil esperado e custos previstos de segurança cibernética relacionados ao produto de IoT (por exemplo, preço de manutenção) e duração e termos de suporte.
    b. Todos os componentes de IoT, incluindo, entre outros, o dispositivo de IoT, que fazem parte do produto de IoT.
    c. Como os critérios da linha de base do produto são atendidos pelo produto de IoT em todos os seus componentes, incluindo quais critérios da linha de base do produto não são atendidos pelos componentes do produto de IoT e por quê (por exemplo, o recurso não é necessário com base na avaliação de risco).
    d. Considerações sobre o design e o suporte do produto relacionadas ao produto de

[15] A documentação discutida neste critério é mantida e controlada pelo desenvolvedor do produto de IoT. O compartilhamento dessas informações pode ser apropriado e pode ser limitado a técnicos autorizados e especialistas em segurança cibernética que buscam mais informações sobre o produto de IoT (por exemplo, na avaliação do produto de IoT para rotulagem, na investigação de uma violação), mas as informações documentadas não se destinam, em todos os casos, a serem compartilhadas diretamente com os consumidores.

IoT, *por exemplo*:

i. Todos os componentes de hardware e software, de todas as fontes (por exemplo, código aberto, propriedade de terceiros, desenvolvido internamente), usados para criar o produto de IoT (ou seja, usados para criar cada componente do produto).
ii. Plataforma de IoT usada no desenvolvimento e na operação do produto de IoT, seus componentes de produto, incluindo a documentação relacionada.
iii. Confiabilidade e proteção dos elementos de software e hardware implementados para criar o produto de IoT e seus componentes (por exemplo, inicialização segura, raiz de confiança do hardware e enclave seguro).
iv. Consideração dos riscos conhecidos relacionados ao produto de IoT e dos possíveis usos indevidos conhecidos.
v. Desenvolvimento seguro de software e práticas de cadeia de suprimentos utilizadas.
vi. Resultados de credenciamento, certificação e/ou avaliação de práticas relacionadas à segurança cibernética.
vii. A facilidade de instalação e manutenção do produto de IoT por um cliente (ou seja, a usabilidade do produto [ISO9241]).

e. Requisitos de manutenção para o produto de IoT, *por exemplo*:
   i. Expectativas de manutenção da segurança cibernética e instruções ou procedimentos associados (por exemplo, plano de gerenciamento de vulnerabilidades/patch).
   ii. Como o desenvolvedor do produto de IoT identifica as partes de suporte autorizadas que podem realizar atividades de manutenção (por exemplo, centros de reparo autorizados).
   iii. Considerações sobre a segurança cibernética do processo de manutenção (por exemplo, como os dados do cliente não relacionados ao processo de manutenção permanecem confidenciais até mesmo para os mantenedores).
f. As políticas e os processos do ciclo de vida do sistema seguro associados ao produto de IoT, **incluindo:**
   i. Etapas adotadas durante o desenvolvimento para garantir que o produto de IoT e seus componentes estejam livres de vulnerabilidades conhecidas e exploráveis.
   ii. O processo de trabalho com fornecedores de componentes e fornecedores terceirizados para garantir que a segurança do produto de IoT e de seus componentes seja mantida durante todo o ciclo de vida suportado.
   iii. Quaisquer considerações após o fim do suporte, como a descoberta de uma vulnerabilidade que afetaria significativamente a segurança, a privacidade ou a proteção dos clientes que

continuam a usar o produto de IoT e seus componentes.

g. As políticas e os processos de gerenciamento de vulnerabilidades associados ao produto de IoT, **incluindo**:
    i. Métodos de recebimento de relatórios de vulnerabilidades (consulte Recepção de informações e consultas abaixo).
    ii. Processos para registrar as vulnerabilidades relatadas.
    iii. Política de resposta a vulnerabilidades relatadas, incluindo o processo de coordenação das atividades de resposta a vulnerabilidades entre fornecedores de componentes e fornecedores terceirizados.
    iv. Política de divulgação de vulnerabilidades relatadas.
    v. Processos para receber notificações de fornecedores de componentes e de terceiros sobre qualquer alteração no status de seus componentes fornecidos, como fim da produção, fim do suporte, status obsoleto (por exemplo, o produto não é mais recomendado para uso) ou inseguranças conhecidas.

Utilitário de segurança cibernética: A geração, a captura e o armazenamento de informações importantes sobre o produto de IoT e seu desenvolvimento (por exemplo, avaliação do produto de IoT e das práticas de desenvolvimento usadas para criá-lo e mantê-lo) podem ajudar a informar o desenvolvedor do produto de IoT sobre a postura real de segurança cibernética do produto.

Recepção de Informações e Consultas

O desenvolvedor de produtos de IoT tem a capacidade de receber informações relevantes para a segurança cibernética e responder a consultas do cliente e de outras pessoas sobre informações relevantes para a segurança cibernética.

1. O desenvolvedor de produtos de IoT pode receber informações relacionadas à segurança cibernética do produto de IoT e de seus componentes e pode responder a consultas relacionadas à segurança cibernética do produto de IoT e de seus componentes de clientes e outros, **incluindo**:
    a. A capacidade do desenvolvedor de produtos de IoT de identificar um ponto de contato para receber informações sobre manutenção e vulnerabilidade (por exemplo, recursos de relatório de bugs e programas de recompensa por bugs) dos clientes e de outras pessoas no ecossistema de produtos de IoT (por exemplo, técnico de reparo agindo em nome do cliente).
    b. A capacidade do desenvolvedor do produto de IoT de receber consultas e responder aos clientes e a outras pessoas no ecossistema do produto de IoT sobre a segurança cibernética do produto de IoT e/ou de seus componentes.

Utilitário de segurança cibernética: À medida que os produtos de IoT são usados pelos clientes, esses clientes podem ter perguntas ou relatos de problemas que podem ajudar a melhorar a segurança cibernética do produto de IoT ao longo do tempo.

Disseminação de Informações

O desenvolvedor de produtos de IoT transmite (por exemplo, para o público) e distribui (por exemplo, para o cliente ou outros no ecossistema de produtos de IoT) informações relevantes para a segurança cibernética.

1. O desenvolvedor do produto de IoT pode transmitir para muitas/todas as entidades por meio de um canal (por exemplo, uma publicação em um canal público, e-mails enviados para todos os endereços registrados dos clientes afetados) para alertar o público e os clientes do produto de IoT sobre informações e eventos relevantes de segurança cibernética durante todo o ciclo de vida do suporte. **No mínimo, essas informações devem incluir**:
    a. Termos de suporte atualizados (por exemplo, frequência de atualizações e mecanismo(s) de aplicação) e aviso de disponibilidade e/ou aplicação de atualizações de software.
    b. Fim do prazo de suporte ou funcionalidade do produto de IoT.
    c. Operações de manutenção necessárias.
    d. Novas vulnerabilidades de dispositivos IoT, detalhes associados e ações de mitigação necessárias por parte do cliente.
    e. Descoberta de violação relacionada a um produto de IoT e seus componentes de produto usados pelos clientes, detalhes associados e ações de mitigação necessárias por parte do cliente (se houver).
2. O desenvolvedor do produto de IoT pode distribuir informações relevantes para a segurança cibernética do produto de IoT e de seus componentes para alertar as entidades apropriadas do ecossistema (por exemplo, fabricantes de componentes de produtos de IoT e/ou entidades de suporte, autoridades comuns de rastreamento de vulnerabilidades, credenciadores e certificadores, organizações de suporte e manutenção de terceiros) sobre informações relevantes para a segurança cibernética, *por exemplo*:
    a. Documentação aplicável capturada durante o projeto e o desenvolvimento do produto de IoT e de seus componentes.[16]
    b. Alertas de segurança cibernética e de vulnerabilidade e informações sobre a resolução de qualquer vulnerabilidade.
    c. Uma visão geral das práticas e proteções de segurança da informação usadas pelo desenvolvedor de produtos de IoT.
    d. Resultados de credenciamento, certificação e/ou avaliação das práticas relacionadas à segurança cibernética do desenvolvedor de produtos de IoT.

[16] Esse subcritério tem o objetivo de indicar que as informações capturadas como parte do recurso de Documentação podem precisar ser comunicadas a entidades específicas (por exemplo, fabricantes de componentes de produtos de IoT e/ou entidades de suporte, autoridades comuns de rastreamento de vulnerabilidades, credenciadores e certificadores, organizações terceirizadas de suporte e manutenção). Na maioria dos casos, esse tipo de documentação só seria compartilhado com as partes interessadas que têm uma finalidade específica para as informações (por exemplo, avaliação de conformidade) e, em geral, não seria compartilhado publicamente ou mesmo com clientes do setor de consumo.

e. Um relatório ou resumo de avaliação de risco para a postura de risco do ambiente de negócios do desenvolvedor de produtos de IoT.

Utilitário de segurança cibernética: À medida que o produto de IoT, seus componentes, ameaças e mitigações mudam, os clientes precisarão ser informados sobre como usar o produto de IoT com segurança.

Educação e Conscientização sobre Produtos

O desenvolvedor de produtos de IoT conscientiza e educa os clientes e outras pessoas no ecossistema de produtos de IoT sobre informações relacionadas à segurança cibernética (por exemplo, considerações, recursos) relacionadas ao produto de IoT e seus componentes.[17]

1. O desenvolvedor de produtos de IoT cria conscientização e fornece educação direcionada aos clientes sobre informações relevantes para a segurança cibernética do produto de IoT e seus componentes, **inclusive**:
    a. A presença e o uso de recursos de segurança cibernética de produtos de IoT, **incluindo, no mínimo**:
        i. Como alterar as definições de configuração e as implicações de segurança cibernética da alteração das configurações, se houver.
        ii. Como configurar e usar a funcionalidade de controle de acesso (por exemplo, definir e alterar senhas).
        iii. Como as atualizações de software são aplicadas e quaisquer instruções necessárias para o cliente sobre como usar a funcionalidade de atualização de software.
        iv. Como gerenciar os dados do dispositivo, incluindo a criação, a atualização e a exclusão de dados no produto de IoT.
    b. Como manter o produto de IoT e seus componentes durante sua vida útil, inclusive após o período de suporte de segurança (por exemplo, fornecimento de atualizações e patches de software) do desenvolvedor do produto de IoT.
    c. Como um produto de IoT e seus componentes podem ser reprovisionados ou descartados com segurança.
    d. Opções de gerenciamento de vulnerabilidades (por exemplo, gerenciamento de configuração e patches e antimalware) disponíveis para o produto de IoT ou seus componentes que podem ser usados pelos clientes.
    e. Informações adicionais que os clientes podem usar para tomar decisões de compra informadas sobre a segurança do produto de IoT (por exemplo, a duração e o escopo do suporte ao produto por meio de atualizações e patches de software).

Utilitário de segurança cibernética: Os clientes precisarão ser informados sobre como usar o dispositivo com segurança para obter os melhores resultados de segurança cibernética para os clientes e o mercado de produtos de IoT para consumidores.

[17] As informações e o conhecimento para desenvolver educação e conscientização eficazes relacionadas a um produto de IoT podem estar no desenvolvedor ou fabricante do componente do produto de IoT. Recomenda-se um ecossistema de educação e conscientização que compartilhe informações sobre a segurança cibernética de IoT, mesmo antes da implantação de um produto de IoT, pois isso ajudará na implementação desse e de outros recursos de segurança cibernética.

3. Considerações sobre o setor de consumo utilizadas para criar o perfil

O NIST usou os conceitos de criação de perfil da linha de base principal do recurso de segurança cibernética do dispositivo de IoT para desenvolver o perfil do consumidor. A primeira etapa foi reunir fontes e outras informações sobre a segurança cibernética de produtos de IoT para consumidores. Em seguida, o NIST usou essas informações para criar o perfil do consumidor usando as fontes, as informações e as conclusões e percepções resultantes.

3.1. Coleta de informações de fontes sobre a segurança cibernética de produtos de IoT para consumidores

O perfil do consumidor foi criado a partir da resposta do NIST à EO 14028, que orientou o NIST a desenvolver recomendações para um programa de rótulo de segurança cibernética de produtos de IoT para consumidores. As recomendações eram mais amplas do que o desenvolvimento de um perfil de consumidor da linha de base principal de IoT, mas o perfil era um elemento-chave dessa tarefa. Portanto, o NIST conseguiu reunir fontes e participar de discussões com partes interessadas externas sobre as necessidades e os objetivos dos clientes de produtos de IoT para consumidores. Ao longo de um ano de eventos, reuniões e outros compromissos, foram coletados centenas de comentários relacionados à rotulagem de segurança cibernética para produtos de IoT para consumidores, muitos dos quais informaram o perfil da linha de base principal para esse setor.

O NIST também analisou o domínio público para identificar vulnerabilidades aplicáveis ao setor de produtos de IoT para consumidores. Essas informações são importantes para determinar uma visão transversal das vulnerabilidades dos produtos de IoT para consumidores que podem servir como base para determinar ameaças e vulnerabilidades. Essas ameaças e vulnerabilidades informam o processo de criação de perfis, especialmente os aspectos de segurança mínima. Tabela 1, reproduzida da *rotulagem de segurança cibernética do consumidor para produtos de IoT: Discussion Draft on the Path Forward* Whitepaper [Path_Forward] lista uma série de vulnerabilidades aplicáveis e bem documentadas, suas categorias de ataque associadas ao MITRE ATT&CK Framework[ATT_CK] e os recursos perfilados que podem ajudar a resolver a vulnerabilidade.[18]

Tabela 1. Exemplo de vulnerabilidades de IoT do consumidor e os recursos relevantes do perfil do consumidor.

Vulnerabilidade	Recursos relevantes do perfil do consumidor
Ataques de variantes de malware Mirai – Usar de autenticação fraca para permitir o carregamento de malware no dispositivo e usar esse dispositivo em ataques DDOS e outros.	

[18] Os recursos identificados não são exaustivos, mas foram incluídos para demonstrar que os recursos de segurança cibernética de suporte, como os detalhados no perfil do consumidor, podem ajudar a mitigar ou evitar as vulnerabilidades identificadas. Por exemplo, um recurso de controle de acesso à interface poderia ter impedido o acesso não autorizado a um dispositivo de IoT.

Vulnerabilidade	Recursos relevantes do perfil do consumidor
Acesso não autorizado ao dispositivo IoT	Identificação de Ativos Controle de Acesso à Interface Disseminação de Informações Educação e Conscientização
O código malicioso pode ser carregado no dispositivo IoT	Atualização de Software Conscientização Sobre o Estado da Segurança Cibernética Educação e Conscientização
Os comandos podem ser iniciados usando o dispositivo	Controle de Acesso à Interface Documentação
Publicação não autorizada de dados de rastreadores de condicionamento físico - Os dados de localização de rastreadores de condicionamento físico de militares foram publicados publicamente, mesmo quando o produto estava configurado para privacidade.	
Vulnerabilidades de aplicativos da Web	Configuração do produto Conscientização Sobre o Estado da Segurança Cibernética Documentação Disseminação de Informações
Vulnerabilidades de aplicativos móveis	Configuração do Produto Conscientização Sobre o Estado da Segurança Cibernética Documentação Disseminação de Informações
Capacidade de reidentificação de dados não identificados	Configuração do Produto Proteção de Dados Documentação
Acesso não autorizado a dados de câmeras de segurança domésticas – O acesso não autorizado a dados e visualizações do interior e exterior de edifícios ocorreu com várias marcas de câmeras de segurança.	
Autenticação fraca	Controle de Acesso à Interface

Vulnerabilidade	Recursos relevantes do perfil do consumidor
Compartilhamento de dados não autorizado	Proteção de Dados Documentação Disseminação de Informações
Não responderam às perguntas e reclamações dos desenvolvedores	Recepção de informações e consultas
Falta de recursos e procedimentos de monitoramento	Identificação de Ativos Configuração do Produto Documentação
Falta de controles de registro/coleta de dados	Identificação de Ativos Configuração do Produto Documentação Disseminação de Informações Educação e Conscientização

O NIST também analisou os padrões existentes, a conformidade e o ecossistema de rotulagem de dispositivos e produtos de IoT para entender onde os outros levaram em conta as considerações dos produtos de IoT do consumidor. Foram analisados cerca de 30 documentos de origem, incluindo leis de segurança cibernética de IoT, catálogos de recursos de segurança cibernética, conjuntos de recursos de linha de base e esquemas de classificação.[19] Todos abordaram especificamente o próprio dispositivo de IoT, mas vários incluíram a nuvem, o aplicativo móvel, o hub ou outros componentes externos em suas considerações como parte de um produto de IoT. Durante os períodos de comentários públicos e discussões com as partes interessadas, a visão mais ampla (ou seja, de produto de IoT versus dispositivo de IoT) foi apoiada, pois o NIST observou um grande consenso sobre a necessidade de incluir todos os componentes de um produto de IoT no escopo de um conjunto estabelecido de recursos de segurança cibernética.

3.2. Avaliação das fontes de segurança cibernética de produtos de IoT para consumidores

Os documentos de origem podem ser comparados mais diretamente com os recursos de suporte técnico e não técnico estabelecidos nas NISTIRs 8259A e 8259B. Dos 30 documentos de origem coletados, uma subamostra de 8 estava mais diretamente relacionada a produtos de IoT para consumidores. Essa subamostra foi comparada com os recursos descritos nas NISTIR 8259A/B, que mostrou que havia um amplo alinhamento com os recursos técnicos, embora alguns recursos

[19] A EO 14028 instruiu o NIST a considerar níveis para as recomendações de rotulagem de IoT para o consumidor, mas a pesquisa do NIST e o feedback subsequente não produziram um conjunto ou uma estrutura clara e eficaz para o desenvolvimento de níveis. As fontes existentes que abordam os níveis não o fizeram com uma visão consensual. Além disso, o NIST ouviu comentários de que as camadas deveriam refletir os níveis crescentes de risco relacionados aos produtos de IoT para consumidores, mas a variedade de casos de uso de IoT para consumidores faz com que o agrupamento desses casos de uso seja baseado no risco, um pré-requisito para classificá-los, uma tarefa que não pôde ser concluída dentro do prazo de um ano para a resposta à EO 14028.

técnicos comuns não encontrados na NISTIR 8259A tenham sido usados para adaptar a linha de base principal ao perfil do consumidor. No entanto, poucos documentos de origem abordaram os recursos não técnicos desenvolvidos com base na NISTIR 8259B. Como os usuários previstos dos dispositivos de IoT para consumidores geralmente não são especialistas em segurança cibernética, esses recursos de suporte não técnicos são essenciais para garantir uma operação segura.

Isso foi confirmado por meio de comentários públicos e feedback verbal ao longo do trabalho para a resposta da EO, que serviu como outra fonte de informações que o NIST utilizou para informar o perfil do consumidor. Por meio dessas fontes, o NIST também ouviu uma série de outras maneiras pelas quais o setor de consumo pode ser diferente do caso geral ou de outros setores. Por exemplo, o gerenciamento de riscos de segurança cibernética de clientes corporativos é geralmente mais estruturado e formalizado em comparação com a abordagem de gerenciamento de riscos de segurança cibernética usada por clientes do setor de consumo. Em geral, as empresas também têm mais acesso à experiência em segurança cibernética do que os consumidores comuns. Essas diferenças e outras percepções têm implicações sobre como os recursos de segurança cibernética devem ser abordados e fornecidos. A Tabela 2 destaca as principais percepções usadas no desenvolvimento do perfil de IoT do consumidor.

Tabela 2. Informações destacadas e principais conclusões do processo de definição do perfil de IoT do consumidor.

Informações Destacadas	Principais Conclusões
As percepções de segurança cibernética para o setor de consumo com base em riscos e vulnerabilidades são semelhantes às do caso de linha de base principal geral. (por exemplo, os listados na Tabela 1)	A maioria dos recursos tem conceitos de segurança cibernética semelhantes à linha de base principal
As diretrizes de segurança cibernética no nível do dispositivo seriam insuficientes com base nas necessidades e nas metas dos clientes para esse setor, incluindo, entre outras, a falta de distinção entre o dispositivo de IoT e os componentes de suporte.	Produto é o nível preferido para as diretrizes de segurança cibernética de IoT para consumidores.
A privacidade e a segurança são preocupações importantes para os produtos de IoT do consumidor, juntamente com a segurança cibernética.	Os recursos de segurança cibernética devem ser projetados para não criar riscos nessas áreas e para apoiar abordagens gerais de mitigação de riscos à privacidade e à segurança.

Informações Destacadas	Principais Conclusões
Não há um conjunto claro e universal de necessidades e metas do consumidor para a segurança cibernética no setor de consumo, e o NIST identificou várias abordagens para atender às necessidades e metas do cliente entre os documentos de origem incluídos na análise do cenário.	Os recursos devem ser baseados em funções de segurança cibernética universalmente aceitas e geralmente aplicáveis.
As necessidades e as metas dos clientes desse setor variam. Os clientes podem ter conhecimentos e habilidades limitados em relação às tecnologias de IoT/TI e às funções de segurança cibernética.	Os fatores humanos relacionados aos recursos de segurança cibernética são fundamentais para mitigar os riscos de segurança cibernética.

Essas percepções e conclusões resultantes levaram o NIST às seguintes considerações sobre um perfil de IoT do consumidor:

1. Ficou claro que muitos dispositivos de IoT para consumidores são suportados por componentes adicionais, como um back-end e/ou aplicativo móvel, que são essenciais para o uso do dispositivo de IoT, a ponto de o dispositivo não poder ser usado de forma significativa sem esses componentes.
2. Além disso, os consumidores domésticos geralmente têm pouco controle sobre esses componentes adicionais. Portanto, ao considerar como a centralização no dispositivo será aplicada ao setor de consumo, o conceito deve se expandir além do dispositivo para incluir o produto completo. Esse escopo pode incluir componentes adicionais como parte de um produto de IoT, inclusive aqueles com os quais o consumidor interage apenas indiretamente (por exemplo, back-end).
3. O perfil do consumidor deve ser implementado no contexto das principais percepções e considerações de privacidade e segurança do setor. No entanto, as considerações de segurança e privacidade são dinâmicas para produtos de IoT para consumidores, devido ao fato de que, mesmo nesse setor específico, os casos de uso de produtos de IoT podem variar significativamente. Pode haver implicações claras de segurança em um produto e em sua operação, mas nem sempre é esse o caso. O mesmo se aplica à privacidade. Isso é exacerbado pelo fato de que diferentes casos de uso podem compartilhar considerações amplas de segurança e/ou privacidade, mas as especificidades de seus impactos e/ou atenuações podem ser muito diferentes. Tudo isso significa que os recursos de segurança cibernética do perfil do consumidor devem oferecer suporte amplo a uma variedade de casos de uso e, ao mesmo tempo, tomar cuidado para não prejudicar essas áreas.
4. As práticas de segurança cibernética dos clientes (ou seja, consumidores domésticos) que estariam gerenciando produtos de IoT para consumidores variam em definição e maturidade. A natureza imprevisível e ad hoc da mitigação de risco do cliente para produtos de IoT para consumidores destaca a necessidade de que práticas de segurança cibernética amplamente úteis e geralmente recomendadas sejam refletidas no perfil.

5. Além disso, uma necessidade importante de segurança cibernética para esse setor são os recursos de segurança cibernética utilizáveis que são implementados para exigir uma configuração e interação mínima/eficiente com o cliente para uso, uma vez que esses clientes não terão conhecimento profundo ou recursos para aproveitar se os recursos não forem utilizáveis para eles.
6. Por fim, padrões, soluções, implementações ou atenuações específicas devem ser usados conforme apropriado para a funcionalidade e o caso de uso de um produto de IoT. Isso significa que nenhum conjunto único de requisitos específicos pode ser aplicável a todos os produtos de IoT para consumidores. Portanto, o perfil do consumidor descreve as diretrizes de segurança cibernética no nível do produto de IoT em termos de resultados a serem alcançados e apoiados pelo produto como um todo, mas pode não se aplicar a todos os componentes do produto de IoT da mesma forma. Alguns componentes podem não ser capazes, ou não precisam, suportar todos os critérios.[20] Esses resultados fornecem orientação para uma variedade de tecnologias e casos de uso, mas permitem flexibilidade na aplicação do perfil do consumidor a produtos específicos de IoT.[21]

O NIST aplicou essas considerações aos recursos de linha de base das NISTIRs 8259A/B para adaptar a abordagem geral de IoT ao setor de consumo. O perfil do consumidor resultante, embora mais diretamente adaptado para o setor, ainda tem a intenção de falar sobre uma ampla gama de tecnologias de IoT, casos de uso e considerações de mitigação de riscos. Portanto, a aplicação do perfil do consumidor a um produto, tipo de produto ou componente de produto de IoT específico pode exigir uma adaptação adicional, mas semelhante, por meio da coleta e consideração de informações, conforme descrito nesta Seção.

[20] Conforme discutido em *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (Critérios recomendados para rotulagem de segurança cibernética para produtos de Internet das Coisas (IoT) para consumidores)*, nem todos os recursos ou subcritérios podem ser aplicados ou suportados da mesma forma por todos os componentes de produtos de IoT. Isso pode ser devido a considerações de risco do produto, desenvolvimento do produto (por exemplo, tarefas de segurança cibernética delegadas por meio de contratos e cadeia de suprimentos), natureza dos componentes para formar o produto (por exemplo, os back-ends podem ser altamente distribuídos) ou limitações dos componentes de IoT (por exemplo, os dispositivos podem ser restritos, os aplicativos de software complementares podem ter acesso e funcionalidade limitados). Considerar isso ao aplicar os recursos e subcritérios a produtos do mundo real (por exemplo, por meio de um mecanismo de avaliação de conformidade) é fundamental para um mercado e um ecossistema de segurança cibernética robustos que possam atender a necessidades e contextos diferentes.

[21] O NIST orienta que aqueles que possuem orientações, padrões ou programas que acreditam apoiar ou se relacionar de alguma forma com alguns ou todos os resultados refletidos nesse perfil devem procurar o Catálogo de Referência Informativa On-line (OLIR) do NIST para obter mais informações sobre como enviar mapeamentos públicos entre seu trabalho e o perfil do consumidor.

Referências

[ATT_CK] The MITRE Corporation (2013) Adversarial Tactics, Techniques, and Common Knowledge. (The MITRE Corporation, Bedford, MA). https://attack.mitre.org/

[EO_Criteria] National Institute of Standards and Technology (2022) Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.24

[IR8259] Fagan M, Megas KN, Scarfone K, Smith M (2020) Atividades fundamentais de segurança cibernética para fabricantes de dispositivos de IoT. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259. https://doi.org/10.6028/NIST.IR.8259

[IR8259A] Fagan M, Megas KN, Scarfone K, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. https://doi.org/10.6028/NIST.IR.8259A

[IR8259B] Fagan M, Marron J, Brady KG, Jr., Cuthill BB, Megas KN, Herold R (2020) IoT Non-Technical Supporting Capability Core Baseline. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259B. https://doi.org/10.6028/NIST.IR.8259B

[ISO9241] International Organization for Standardization/International Electrotechnical Commission (2018) ISO 9241-11:2018 Ergonomia da interação homem-sistema - Parte 11: Usabilidade: Definições e conceitos (ISO Genebra, Suíça). Disponível em https://www.iso.org/standard/63500.html

[Path_Forward] Instituto Nacional de Padrões e Tecnologia (2021) Rotulagem de segurança cibernética do consumidor para produtos de IoT: Rascunho de discussão sobre o caminho a seguir. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD). Disponível em: https://www.nist.gov/document/draft-paper-consumer-cybersecurity-labeling-iot-products-discussion-draft-path-forward

Apêndice A. Glossário

produto de IoT para o consumidor
Produtos de IoT destinados ao uso pessoal, familiar ou doméstico.

linha de base principal
Um conjunto de recursos de segurança cibernética de dispositivos e recursos de suporte não técnicos necessários para dar suporte a controles comuns de segurança cibernética que protegem os dispositivos do cliente e os dados, sistemas e ecossistemas dos dispositivos.

recurso de segurança cibernética do produto
Recursos ou funções de segurança cibernética que os dispositivos de computação fornecem por meio de seus próprios meios técnicos (ou seja, hardware e software do dispositivo). [IR8259]

> *Observação:* Esse termo é sinônimo de recursos de segurança cibernética *do dispositivo* , conforme definido na NISTIR 8259, mas tem como escopo um produto de IoT, conforme definido neste documento, em vez de apenas o dispositivo de IoT.

Dispositivo de IoT
Dispositivos que têm pelo menos um transdutor (sensor ou atuador) para interagir diretamente com o mundo físico e pelo menos uma interface de rede (por exemplo, Ethernet, Wi-Fi, Bluetooth) para fazer interface com o mundo digital.

Produto de IoT
Um dispositivo ou dispositivos de IoT e quaisquer componentes adicionais do produto (por exemplo, back-end, aplicativo móvel) necessários para usar o dispositivo de IoT além dos recursos operacionais básicos.

Componente de produto de IoT
Um dispositivo de IoT ou outro equipamento ou serviço digital (por exemplo, back-end, aplicativo móvel) usado para criar produtos de IoT.

recurso de suporte não técnico
Os recursos de suporte não técnico são ações que uma organização realiza para apoiar a segurança cibernética de um dispositivo de IoT.