NISTIR 8259

Atividades Fundamentais de Cibersegurança para Fabricantes de Dispositivos IoT

Michael Fagan
Katerina N. Megas
Karen Scarfone
Matthew Smith

Esta publicação está disponível gratuitamente em:
https://doi.org/10.6028/NIST.IR.8259pt

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8259

Atividades Fundamentais de Cibersegurança para Fabricantes de Dispositivos IoT

Michael Fagan
Katerina N. Megas
Divisão de Cibersegurança Aplicada
Laboratório de Tecnologia da Informação

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

Matthew Smith
Huntington Ingalls Industries
Annapolis Junction, MD

Esta publicação está disponível gratuitamente em:
https://doi.org/10.6028/NIST.IR.8259pt

Maio 2020

Departamento de Comércio dos EUA
Wilbur L. Ross, Jr., Secretário

Instituto Nacional de Padrões e Tecnologia
Walter Copan, Diretor do NIST e Subsecretário de Comércio para Padrões e Tecnologia

Relatório Interno ou Interagências 8259 do Instituto Nacional de Normas e Tecnologia
40 páginas (Maio 2020)

Esta publicação está disponível gratuitamente em:
https://doi.org/10.6028/NIST.IR.8259pt

Os comentários sobre esta publicação podem ser enviados para:

Instituto Nacional de Normas e Tecnologia
A/C: Divisão de Segurança Cibernética Aplicada, Laboratório de Tecnologia da Informação
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
E-mail: iotsecurity@nist.gov

Disclaimer

This document was translated by the U.S. Department of State, Office of Language Services with support from the Digital Connectivity and Cybersecurity Partnership (DCCP).

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.8259.

Relatórios sobre Tecnologia de Sistemas Informáticos

O Laboratório de Tecnologia da Informação (ITL) do Instituto Nacional de Normas e Tecnologia (NIST) promove a economia e o bem-estar público dos EUA, fornecendo liderança técnica para a infraestrutura de medição e normas da Nação. O ITL desenvolve testes, métodos de testes, 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 normas e diretrizes gerenciais, administrativos, técnicos e físicos para a segurança economicamente viável e a privacidade de outras informações, além das relacionadas à segurança nacional em sistemas federais de informação.

Resumo

Os dispositivos da Internet das Coisas (IoT) muitas vezes não possuem recursos de segurança cibernética de acordo com os dispositivos que os seus clientes — organizações e indivíduos — querem usar para ajudar a mitigar riscos de segurança cibernética. Os fabricantes podem ajudar os seus clientes incrementando o nível de segurança dos dispositivos IoT que produzem, fornecendo a funcionalidade e as informações necessárias relacionadas à cibersegurança que efetivamente seus clientes precisam ter. Esta publicação descreve as atividades recomendadas relacionadas à segurança cibernética que os fabricantes devem considerar implementar antes que os seus dispositivos IoT sejam vendidos aos clientes. Tais atividades fundamentais de cibersegurança podem ajudar os fabricantes a diminuir os esforços envidados pelos clientes no sentido de manter a segurança cibernética desejada, o que, por sua vez, reduz a prevalência e a gravidade das adulterações dos dispositivos IoT e os ataques realizados usando dispositivos comprometidos.

Palavras-chave

risco de cibersegurança; Internet das Coisas (IoT); fabricação; gestão de risco; mitigação de riscos; dispositivos de computação protegíveis; desenvolvimento de software.

Reconhecimentos

Os autores desejam agradecer a todos os colaboradores desta publicação, incluindo os participantes em workshops e outras sessões interativas; os indivíduos e organizações dos setores público e privado, incluindo fabricantes de vários setores da indústria, além de diversas organizações comerciais de fabricantes que forneceram feedback sobre o ensaio preliminar e os esboços de comentários públicos. Agradecemos também aos colegas do NIST que nos trouxeram informações e feedback importantes. Queremos agradecer, especialmente, a todos os integrantes do Programa de Cibersegurança para IoT, Barbara Cuthill e Jeff Marron, e à equipe do Projeto de Implementação do NIST FISMA por sua ajuda na editoração deste trabalho.

Público-alvo

Os fabricantes de dispositivos IoT são o público-alvo desta publicação. A publicação também pode ajudar os clientes que usam os dispositivos IoT a melhor entenderem os recursos de

cibersegurança que são oferecidos e quais as informações sobre cibersegurança que os fabricantes podem proporcionar.

Informações sobre marcas registradas

Todas as marcas registradas e marcas comerciais pertencem às suas respectivas organizações.

Aviso de divulgação de patente

AVISO: A ITL solicitou que os detentores de pedidos de patentes cujo uso possa ser necessário para o cumprimento das diretrizes ou requisitos desta publicação, divulguem tais pedidos de patente à ITL. No entanto, os detentores de patentes não são obrigados a responder aos pedidos da ITL por patentes, e a ITL não realizou uma pesquisa de patentes para identificar quais patentes (se houver) se aplicam a esta publicação.

Até a data desta publicação e das subsequentes solicitações para identificação de pedidos de patentes cujo uso possa ser necessário para o cumprimento das diretrizes ou requisitos desta publicação, nenhum pedido de patente foi identificad0 como sendo da ITL.

Nenhuma declaração foi feita pela ITL ou está implícita de que as licenças não são necessárias para evitar violação de patente no uso desta publicação.

Síntese

Os fabricantes estão criando um volume e uma variedade impressionante de dispositivos prontos para a Internet, amplamente conhecidos como Internet das Coisas (IoT). Muitos dispositivos IoT não se enquadram nas definições padrão de dispositivos de tecnologia da informação (TI) que são usadas como base para definir recursos de cibersegurança (ex.: smartphones, servidores, laptops). Os dispositivos IoT no escopo desta publicação têm pelo menos um transdutor (sensor ou atuador) para interagir diretamente com o mundo físico, e pelo menos uma interface de rede (ex.: Ethernet, Wi-Fi, Bluetooth, Evolução de Longo Prazo [LTE], Zigbee, e Ultra-Wideband [UWB]) para fazer a interface com o mundo digital. No âmbito desta publicação, os dispositivos IoT podem funcionar independentemente, embora possam ser dependentes de outros dispositivos específicos (ex.: um hub IoT) ou sistemas (ex.: uma nuvem) para alguma funcionalidade.

Muitos dispositivos IoT têm funcionalidade de computação, armazenamento de dados e conectividade de rede, juntamente com a funcionalidade associada a equipamentos que anteriormente não tinham funções de computação (ex.: aparelhos inteligentes). Por sua vez, essas funções permitem novas eficiências e recursos tecnológicos para os equipamentos, como acesso remoto para monitoramento, configuração e solução de problemas. A IoT também pode permitir a coleta e análise de dados sobre o mundo físico e usar os resultados para uma tomada de decisão mais informada, alterar o ambiente físico e antecipar eventos futuros [1].

Os dispositivos IoT são adquiridos e usados por muitos clientes: pessoas físicas, empresas, agências governamentais, instituições de ensino e outras organizações. Infelizmente, os dispositivos IoT geralmente não possuem recursos de dispositivo que os clientes possam usar para ajudar a mitigar os riscos de segurança cibernética, como a funcionalidade que eles normalmente esperam ter nos seus desktops, laptops, smartphones, tablets e outros dispositivos de TI. Por esta razão, os clientes de dispositivos IoT talvez precisem selecionar, implementar e gerenciar controles adicionais ou novos de segurança cibernética, ou alterar os controles que já possuem. Para agravar esse problema, talvez eles não saibam que precisam alterar os processos existentes para acomodar as características exclusivas da IoT. Como resultado, muitos dispositivos IoT não estão protegidos contra ameaças evolutivas, fazendo com que os invasores possam comprometer mais facilmente os dispositivos IoT, usando-os para prejudicar os clientes e realizar atos nefastos (ex.: ataques distribuídos de negação de serviço [DDoS]) contra outras organizações.[1]

O objetivo desta publicação é fornecer recomendações aos fabricantes para melhorar a *segurança* dos dispositivos IoT por eles fabricados. Isso significa que os dispositivos IoT oferecem *recursos de cibersegurança dos dispositivos* - isto é, recursos por intermédio dos seus próprios meios técnicos (ex.: hardware e software de dispositivo) - que os clientes, sejam eles organizações ou

[1] Em 2017, Ordem Executiva 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [Fortalecendo a Cibersegurança das Redes Federais e Infraestrutura Crítica] [2], foi emitida para melhorar a postura e recursos cibernéticos da Nação face à intensificação das ameaças. A Ordem Executiva encarregou o Departamento de Comércio e o Departamento de Segurança Interna de criar o Enhancing Resilience Against Botnets Report [Relatório para Reforçar a Ciber-Resiliência Contra Botnets] [3] para determinar como impedir o uso de botnets pelo invasor para realizar ataques DDoS. O relatório continha vários itens de ação, e esta publicação cumpre dois deles: criar uma linha de base de recursos de segurança cibernética para dispositivos IoT e publicar práticas de segurança cibernética para fabricantes de dispositivos IoT.

indivíduos, precisam para proteger os dispositivos quando usados em sistemas e ambientes. Os fabricantes de dispositivos IoT muitas vezes precisarão realizar certas ações ou fornecer serviços que os seus clientes esperam e precisam para que possam planejar a manutenção da cibersegurança do dispositivo em seus sistemas e ambientes. Usando esta publicação como referência, os fabricantes de dispositivos IoT aprenderão como podem ajudar os seus clientes, analisando atentamente quais os recursos de cibersegurança que devem fazer parte do design dos dispositivos IoT por eles fabricados, para que os clientes possam melhor gerenciar os riscos de segurança cibernética.

Esta publicação descreve seis atividades básicas de segurança cibernética recomendadas que devem ser consideradas e implementadas pelos fabricantes com o intuito de melhorar a segurança dos novos dispositivos IoT. Quatro das seis atividades afetam principalmente as decisões e ações realizadas pelo fabricante antes de um dispositivo ser comercializado (pré-mercado), e as duas atividades restantes afetam as decisões e ações após a venda do dispositivo (pós-mercado). A execução de todas as seis atividades pode ajudar os fabricantes a fornecer aos seus clientes dispositivos IoT que oferecem suporte os esforços de cibersegurança, assim reduzindo a prevalência e a gravidade das adulterações, bem como os ataques quando dispositivos IoT comprometidos são utilizados. A intenção é encaixar essas atividades dentro do atual processo de desenvolvimento do fabricante, sendo que elas já podem estar sendo parcial ou totalmente executadas dentro do processo vigente.

Observe que esta publicação tem como objetivo informar sobre a fabricação de novos dispositivos, não sendo direcionada a dispositivos já produzidos ou em produção, embora algumas informações também se apliquem a tais dispositivos.

Atividades com principal impacto na fase pré-mercado

- **Atividade 1: Identificar os prováveis clientes e usuários e definir os possíveis casos de uso.** É importante identificar os prováveis clientes e usuários dos dispositivos IoT, bem como os casos de uso dos usuários finais no início do processo de design para melhor determinar os recursos de cibersegurança que devem ser implementados nos dispositivos e como implementá-los.
- **Atividade 2: Pesquisar as necessidades e objetivos de cibersegurança do cliente.** Para os clientes, a exposição ao risco é o elemento decisório que impulsiona as suas necessidades e objetivos de cibersegurança. Os fabricantes não podem entender completamente ou antecipar todos os riscos dos seus clientes. No entanto, eles podem tornar os seus dispositivos minimamente seguros para que possam ser utilizados pelos clientes que compram o produto esperando que ele seja consistente com os supostos casos de uso.
- **Atividade 3: Determinar como atender às necessidades e objetivos do cliente.** Os fabricantes podem determinar como devem atender às necessidades e objetivos dos seus clientes, fazendo com que os dispositivos IoT proporcionem recursos de cibersegurança específicos para ajudar os clientes a mitigar esse tipo de risco. Inicialmente, para que o dispositivo ideal seja identificado devido à sua capacidade de cibersegurança, viabilizamos uma publicação complementar, o NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [*Linha de base do núcleo para recursos de cibersegurança dos*

dispositivos IoT] [4], que consiste em um conjunto de recursos de cibersegurança que os clientes provavelmente necessitarão para cumprir as suas necessidades e objetivos.

- **Atividade 4: Planejar o suporte adequado às necessidades e objetivos do cliente.** Os fabricantes podem ajudar a tornar os seus dispositivos IoT mais seguros, provisionando adequadamente os recursos de hardware e software para que os requisitos de cibersegurança sejam devidamente atendidos. Eles também devem considerar os recursos de negócios que são necessários para apoiar o desenvolvimento e o suporte contínuo aos dispositivos IoT, com o intuito de atender às necessidades e objetivos do cliente (ex.: práticas de codificação seguras, resposta a vulnerabilidades e correção de falhas).

Atividades com principal impacto na fase pós-mercado

- **Atividade 5: Definir abordagens para comunicação com os clientes.** Muitos clientes se beneficiarão de uma comunicação mais clara por parte dos fabricantes sobre os riscos de segurança cibernética envolvendo os dispositivos IoT que estão sendo ou já foram comercializados. A comunicação pode ser direcionada exclusivamente ao cliente ou a terceiros agindo em nome do cliente, como um provedor de serviços de Internet ou de serviços de segurança gerenciados, dependendo do contexto e funções.
- **Atividade 6: Decidir o que comunicar aos clientes e como fazê-lo.** Existem várias opções que podem ser consideradas sobre qual o tipo de informação o fabricante deve comunicar aos clientes sobre determinado produto de IoT e qual o método de comunicação que deve ser usado. Exemplos de tópicos:
  - Suposições do fabricante relacionadas ao risco de cibersegurança ao criar o design e desenvolver o dispositivo.
  - Expectativas sobre suporte e vida útil, tais como prazo esperado para continuação do suporte técnico, processo de orientação até o fim da vida útil do dispositivo, quais as funções do dispositivo que permanecerão em vigor após o fim da vida útil, como os clientes podem se comunicar com o fabricante sobre vulnerabilidades identificadas durante e após o prazo de suporte do dispositivo, e como os clientes podem manter-se seguros após o vencimento do suporte e fim da vida útil do dispositivo
  - Composição e recursos do dispositivo, como informações sobre o software, hardware, serviços, funções e tipos de dados do dispositivo
  - Atualizações do software – informar se as atualizações estarão disponíveis, além de quando, como e por quem serão enviadas, e como os clientes podem verificar a origem e o conteúdo de uma atualização de software
  - Opções para desativar o dispositivo, como o cliente pode transferir com segurança as propriedades do dispositivo, e se o cliente pode torná-lo inoperante para ser descartado
  - Recursos de cibersegurança proporcionadas pelo dispositivo, bem como funções de cibersegurança proporcionadas por um dispositivo relacionado ou por um serviço ou sistema do fabricante

Tabela de Conteúdo

Lista dos Apêndices

1 Introdução

1.1 Propósito e Escopo

Esta publicação tem como objetivo oferecer recomendações aos fabricantes no sentido de aumentar o nível de *segurança* dos dispositivos da Internet das Coisas (IoT) por eles fabricados. Isso significa que os dispositivos IoT oferecem recursos de cibersegurança—isto é, recursos por intermédio dos seus próprios meios técnicos próprios (ex.: hardware e software do dispositivo) - que os clientes, sejam eles organizações ou indivíduos, precisam para proteger os dispositivos quando usados em sistemas e ambientes. Os fabricantes de dispositivos IoT muitas vezes precisarão realizar certas ações ou fornecer serviços que os seus clientes esperam e precisam para que possam planejar a manutenção da cibersegurança do dispositivo em seus sistemas e ambientes. Usando esta publicação como referência, os fabricantes de dispositivos IoT aprenderão como podem ajudar os seus clientes, analisando atentamente quais os recursos de cibersegurança que devem fazer parte do design dos dispositivos IoT por eles fabricados para que os clientes possam melhor gerenciar os riscos de segurança cibernética. Também devem refletir sobre quais as ações ou serviços necessários para oferecer suporte à segurança do dispositivo IoT para efetivamente atender às necessidades dos seus clientes.

Esta publicação destina-se a abordar uma ampla gama de dispositivos IoT. Os dispositivos IoT no escopo desta publicação têm pelo menos um transdutor (sensor ou atuador) para interagir diretamente com o mundo físico, e pelo menos uma interface de rede (ex.: Ethernet, Wi-Fi, Bluetooth, Evolução de Longo Prazo [LTE], Zigbee, e Ultra-Wideband [UWB]) para fazer a interface com o mundo digital. Os componentes de um dispositivo, como um processador ou sensor que transmite dados para uma estação-base[2] construída para esse fim, que não podem funcionar por conta própria estão fora do âmbito desta publicação.

Alguns dispositivos IoT podem depender de outros dispositivos específicos (ex.: um hub de IoT) ou sistemas (ex.: uma nuvem) para alguma funcionalidade. Os dispositivos IoT serão usados em sistemas e ambientes com muitos outros dispositivos e componentes, alguns dos quais podem ser dispositivos IoT, enquanto outros podem ser equipamentos convencionais de tecnologia da informação (TI). Todas as partes e funções dentro do ecossistema da IoT, além dos próprios dispositivos IoT e das funções do fabricante relacionadas à segurança cibernética desses dispositivos, estão fora do escopo desta publicação.

Esta publicação tem como objetivo informar a fabricação de novos dispositivos e não dispositivos que já estão em produção, embora algumas das informações também possam se aplicar a tais dispositivos.

[2] Em ambos os casos, esses componentes devem ser usados juntamente com outros componentes para formar um dispositivo IoT, e podem desempenhar um papel importante na segurança de um dispositivo IoT (Leia a Seção 3.4). Já que o foco desta publicação é a segurança dos dispositivos IoT para os propósitos do cliente, alguns ou todos os conceitos discutidos podem não se aplicar aos componentes.

Os leitores não precisam ter conhecimento técnico da composição e dos recursos dos dispositivos IoT, mas pressupõe-se que tenham um conhecimento básico dos princípios de segurança cibernética.

1.2 Estrutura da Publicação

O restante desta publicação está organizado nas seguintes seções e apêndices:

- • A seção 2 oferece um background sobre como os fabricantes desempenham um papel importante para garantir o nível de segurança dos dispositivos IoT para os seus clientes, isto é, quais as áreas de mitigação de risco de cibersegurança os clientes precisam abordar, e entender como o dispositivo pode oferecer suporte para as áreas em questão.
- As Seções 3 e 4 descrevem atividades que os fabricantes devem considerar implementar antes que os seus dispositivos IoT sejam vendidos aos clientes, para que possam incrementar a questão da segurança.
  - A seção 3 inclui atividades que impactam principalmente os esforços de segurança do fabricante antes da venda do dispositivo. As atividades da Seção 3 são: identificar os clientes em potencial e definir os casos de uso esperados, pesquisar as necessidades e objetivos de cibersegurança do cliente, determinar como atender às necessidades e objetivos do cliente e planejar o suporte adequado.
  - A Seção 4 inclui atividades que impactam principalmente os esforços de segurança do fabricante após a venda do dispositivo. As atividades da Seção 4 são: definir abordagens para se comunicar com os clientes em relação à segurança cibernética dos dispositivos IoT, decidir o que comunicar aos clientes, e como fazê-lo.
- A Seção 5 apresenta uma conclusão para esta publicação.
- A seção Referências lista as referências contidas nesta publicação.
- O apêndice A fornece uma lista de sigla e abreviações.
- O apêndice B contém um glossário de termos selecionados usados nesta publicação.

2 Contexto

Esta seção proporciona uma visão geral dos conceitos básicos necessários para se compreender o restante da publicação.

Do ponto de vista do fabricante, a fase *pré-mercado* do ciclo de vida de um dispositivo IoT abrange o que o fabricante faz *antes* do marketing e venda do dispositivo aos clientes. Qualquer decisão do fabricante referente a um dispositivo IoT após a sua venda, por exemplo, lidar com vulnerabilidades, viabilizar recursos atualizados, novos dispositivos, ou informações de segurança cibernética aos clientes, será considerada como parte da fase *pós-mercado.* Os fabricantes são mais propensos a identificar e incorporar planos para os recursos de cibersegurança para os seus dispositivos logo no início da fase pré-mercado. Ao final da fase pré-mercado, fica mais complicado e dispendioso fazer alterações na implementação ou no design, o que pode atrasar o lançamento do dispositivo. Uma vez que um dispositivo foi lançado no mercado, muitas mudanças de segurança cibernética podem não ser mais viáveis devido a restrições de hardware, como também as mudanças que ainda podem ser realizadas talvez sejam mais caras e difíceis do que se tivessem sido feitas na fase pré-mercado.

As seções 3 e 4 desta publicação descrevem as atividades de segurança cibernética e o planejamento relacionado que os fabricantes devem considerar implementar durante a fase pré-mercado de um dispositivo IoT. A Seção 3 abrange atividades que impactam principalmente outras atividades pré-mercado, enquanto a Seção 4 discute atividades que impactam principalmente as atividades pós-mercado. As atividades nas seções 3 e 4 se concentram nas principais atividades de cibersegurança e representam um subconjunto do que os fabricantes necessitam fazer durante o processo de desenvolvimento de produtos, mas não são informações abrangentes. Por exemplo, os fabricantes também terão mais facilidade para criar o design e produzir dispositivos IoT seguros se garantirem que a sua força de trabalho possui as habilidades necessárias para realizar as atividades nas Seções 3 e 4.

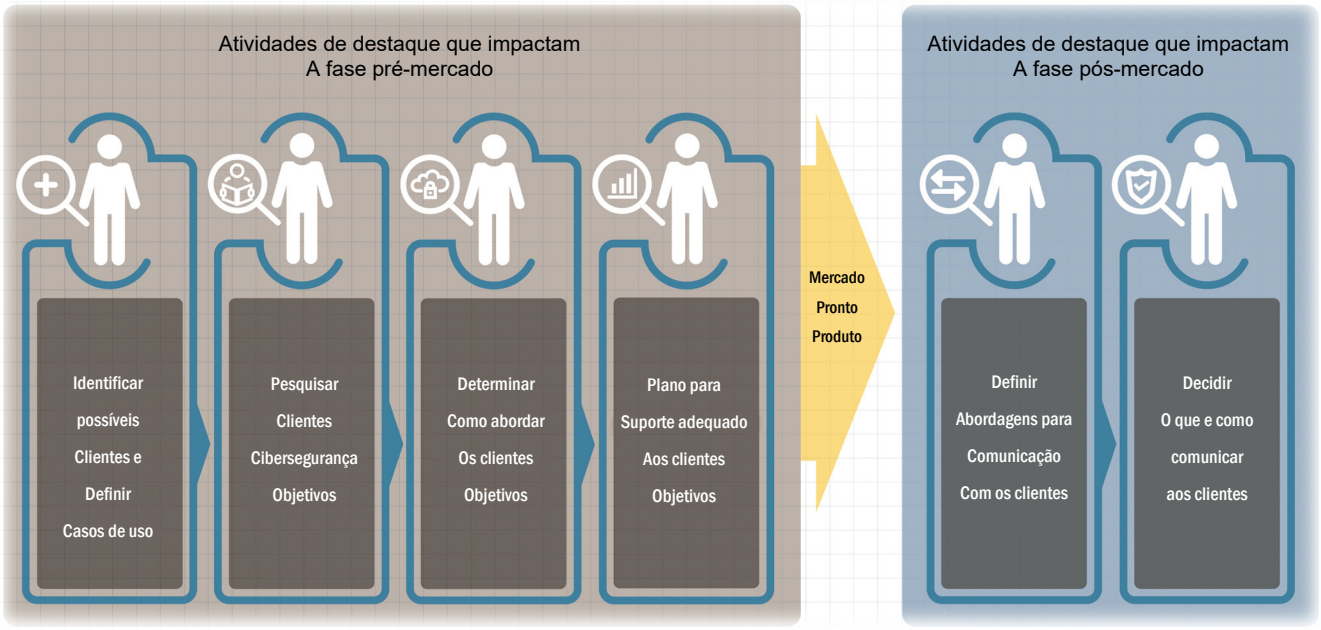

Figura 1: Atividades discutidas nesta publicação agrupadas por fase de impacto

Figure 1 mostra as atividades fundamentais de cibersegurança abordadas nesta publicação, organizadas de acordo com a fase em que os resultados das atividades serão utilizados para aumentar a segurança do dispositivo. Conforme indicado na figura, as atividades destacadas para cada fase se agregam uma à outra dentro desta fase, de modo que cada atividade pré-mercado será construída de acordo com os resultados das atividades anteriores. Embora as atividades destacadas que afetam a fase pós-mercado possam usar artefatos e resultados de atividades pré-mercado, elas também podem recorrer a outras fontes de orientação e informação. O momento em que um dispositivo é considerado como tendo "lançado no mercado" varia de acordo com o produto, fabricante e circunstância, mas esse momento é definido quando um dispositivo fabricado não está mais sob o controle do fabricante (ou seja, quando foi lançado para um intermediário, como um varejista, ou para clientes finais). As atividades que afetam principalmente a fase pós-mercado, devem ser planejadas para ter início na fase pré-mercado, pois a intenção deve ser garantir a segurança dos dispositivos IoT após ou no momento em que são vendidos (ex.: informando aos clientes como o dispositivo pode ajudar a atender necessidades e objetivos de cibersegurança, que pode ou não incluir riscos e objetivos de mitigação).

Melhorar a segurança de um dispositivo IoT para clientes significa ajudá-los a cumprir objetivos de mitigação de risco, o que envolve a identificação e abordagem de um conjunto de áreas ligadas a esse tópico. Mesmo os clientes sem objetivos formais de mitigação de risco, como consumidores domésticos, muitas vezes têm metas informais e indiretas de segurança cibernética, isto é, fazer com que o dispositivo IoT forneça a funcionalidade desejada conforme o esperado (ex.: automaticamente), que depende de alguma maneira da abordagem de áreas de mitigação de risco. Com base em uma análise das publicações NIST disponíveis, como o SP 800-53 [5] o Cybersecurity Framework [6] e as características dos dispositivos IoT, o NISTIR 8228 [7] identificou áreas de mitigação de risco comuns para dispositivos IoT como:

- **Gestão de ativos:** Manter um inventário atual e preciso de todos os dispositivos IoT e suas características relevantes ao longo dos ciclos de vida dos dispositivos, visando usar essas informações para fins de gerenciamento de risco de cibersegurança. Ter a capacidade de distinguir cada dispositivo IoT de todos os outros é necessário para as outras áreas comuns de mitigação de risco - gerenciamento de vulnerabilidades, gerenciamento de acesso, proteção de dados e detecção de incidentes.
- **Gerenciamento de vulnerabilidades:** Identificar e mitigar vulnerabilidades conhecidas no software do dispositivo IoT ao longo dos ciclos de vida dos dispositivos, com o intuito de reduzir a probabilidade e facilidade de exploração e comprometimento. As vulnerabilidades podem ser eliminadas instalando-se atualizações (ex.: patches) e alterando os ajustes de configuração. As vulnerabilidades podem ser eliminadas instalando-se atualizações (ex.: patches) e alterando os ajustes de configuração. As atualizações também podem corrigir problemas operacionais do dispositivo IoT, o que pode melhorar a disponibilidade, confiabilidade, desempenho e outros aspectos referentes à operação do dispositivo. Geralmente, os clientes querem alterar as configurações de um dispositivo por várias razões, incluindo a segurança cibernética, interoperabilidade, privacidade e usabilidade.
- **Gerenciamento de acesso:** Impedir acesso físico e lógico impróprios e não autorizados, uso e administração de dispositivos IoT ao longo dos ciclos de vida dos dispositivos por pessoas, processos e outros dispositivos de computação. Limitar o acesso a interfaces reduz a superfície de ataque do dispositivo, dando aos invasores menos oportunidades de comprometê-lo.
- **Proteção de dados:** Impedir o acesso e a adulteração de dados em repouso ou em trânsito que podem expor informações confidenciais ou permitir a manipulação ou interrupção das operações do dispositivo IoT durante todo o seu ciclo de vida.
- **Detecção de Incidentes:** Monitorar e analisar a atividade do dispositivo IoT para detectar sinais de incidentes envolvendo a segurança do dispositivo e dos dados em todo o ciclo de vida do dispositivo. Esses sinais também podem ser úteis na investigação de adulterações e na solução de certos problemas operacionais.

Os fabricantes de dispositivos IoT podem abordar essas áreas, incorporando recursos de cibersegurança de dispositivos correspondentes em seus próprios dispositivos IoT. Por sua vez, os clientes terão menos problemas para proteger os dispositivos, já que os recursos do dispositivo IoT estarão mais bem alinhados às expectativas do cliente. Muitas áreas só podem ser efetiva e eficientemente abordadas usando-se recursos de cibersegurança integrados aos dispositivos, em vez dos clientes terem que providenciar tais recursos por si próprios.

As seções 3 e 4 do NISTIR 8228 [7] discutem considerações adicionais relacionadas à segurança cibernética às quais os fabricantes devem estar atentos ao identificar os recursos de cibersegurança proporcionados pelos dispositivos IoT. Além disso, as Tabelas 1 e 2 na Seção 4 do NISTIR 8228 listam deficiências comuns na segurança cibernética dos dispositivos IoT, e explicam como elas podem impactar negativamente os clientes, fornecendo um raciocínio lógico para explicar a necessidade de se ter cada recurso e elemento-chave na linha de base definida na publicação complementar, NISTIR 8259A, *IoT Device Cybersecurity Core Baseline* [Linha de base do núcleo de cibersegurança dos dispositivos IoT] [4].

Em se tratando de outros tipos de risco, como privacidade,[3] segurança, confiabilidade ou resiliência, muitos dispositivos IoT precisam ser gerenciados simultaneamente com os riscos de cibersegurança, já que o efeito de lidar com um tipo de risco pode impactar vários outros. Um exemplo disso é garantir que, quando um dispositivo falhar, que seja de uma maneira segura. Apenas os riscos de cibersegurança são discutidos nesta publicação. Os leitores interessados em entender melhor outros tipos de riscos e sua relação com a cibersegurança podem se beneficiar ao lerem a publicação SP 800-82 Revisão 2, Sugerimos que os leitores interessados em entender melhor outros tipos de riscos e sua relação com a cibersegurança, leiam a publicação SP 800-82 Revisão 2, *Guide to Industrial Control Systems (ICS) Security* [Guia para Segurança de Sistemas de Controle Industrial (ICS)] [8] e o NIST SP 1500-201, *Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0* [Volume 1, Visão Geral, Versão 1.0] do Grupo de Trabalho Público de Sistemas Ciber-Físicos[9].

[3] Uma série de esforços de privacidade atuais e recentes, incluindo o NIST Privacy Framework v1.0 (https://www.nist.gov/privacy-framework), provavelmente conterá informações sobre os recursos do dispositivo IoT considerados necessários para oferecer suporte à privacidade. Embora a linha de base do núcleo inclua recursos de cibersegurança de dispositivos que também oferecem suporte à privacidade, como proteger a confidencialidade dos dados, ela não inclui recursos para dispositivos não relacionados à cibersegurança que ofereçam suporte à privacidade.

3 Atividades do fabricante que impactam a fase de pré-mercado do dispositivo IoT

Os fabricantes devem considerar implementar as atividades fundamentais de cibersegurança descritas nesta seção, com o intuito de melhorar o nível de segurança do dispositivo IoT para os clientes (ex.: aumentar o número ou eficácia dos recursos de cibersegurança do dispositivo IoT conforme a expectativa do cliente). As atividades devem ser realizadas paralelamente ou dando prosseguimento a outras atividades pré-mercado empreendidas pelo fabricante, e que impactarão principalmente tais atividades pré-mercado. Algumas atividades podem ter objetivos mais amplos do que a segurança cibernética (ex.: explorar clientes potenciais e casos de uso). Os esforços não precisam ser duplicados, e os artefatos de todas as atividades pré-mercado podem servir para informar quais medidas específicas devem serem tomadas no tocante à segurança cibernética. Quanto mais integradas essas atividades sugeridas forem com outras atividades pré-mercado, melhor será a segurança cibernética planejada e implementada nos dispositivos IoT.

3.1 Atividade 1: Identificar clientes potenciais e definir possíveis casos de uso

Identificar clientes potenciais para um dispositivo IoT no início do processo de design é vital para se determinar como e quais os recursos de segurança cibernética do dispositivo devem ser implementados. Por exemplo, uma grande empresa pode precisar de um dispositivo para integração com os seus servidores de gerenciamento de log, mas isso não seria necessário para um cliente doméstico típico. Os fabricantes podem responder as seguintes perguntas:

1. **1. Qual o tipo de pessoa seria um cliente potencial para esse dispositivo?** (ex.: músicos, pequenos empresários, ciclistas, policiais, chefs, construtores civis, alunos da pré-escola, engenheiros elétricos)
2. **2. Qual o tipo de organização seria um cliente potencial para esse dispositivo?** (ex.: usuários domésticos, pequenas empresas de varejo, grandes hospitais, empresas de energia com fazendas solares, instituições de ensino com ônibus)

Os clientes são os indivíduos ou organizações que compram e implantam um dispositivo IoT e geralmente agem como administradores do dispositivo para fins de cibersegurança, fazendo uso dos recursos para atender às suas necessidades e objetivos. Além dos clientes, alguns dispositivos IoT podem ter outros usuários que não compraram o equipamento, porém, interagem com o dispositivo e podem também ter necessidades e objetivos de cibersegurança. A maioria dos clientes age como um usuário dos dispositivos IoT adquiridos, mas nem todos os dispositivos IoT têm usuários além do cliente. O restante desta publicação terá como enfoque o cliente, pois todos os dispositivos IoT têm um cliente. Porém, conforme discutiremos a seguir, os fabricantes devem considerar *como* um dispositivo pode ser usado também no caso de existirem outros usuários além do cliente.

Outro passo inicial no design do dispositivo IoT é definir casos de uso esperados para o dispositivo com base nos clientes potenciais. Para ajudar a definir um caso de uso, os fabricantes podem responder as seguintes perguntas, com base em como antecipam que o dispositivo será razoavelmente implantado e usado:

1. **Como o dispositivo será usado?** (ex.: para um ou múltiplos propósitos; incorporado em outro dispositivo ou não, usuário/cliente único ou vários usuários; uso pessoal ou comercial)
2. **Onde o dispositivo será usado geograficamente?** (ex.: países, jurisdições dentro dos países)
3. **Em quais ambientes físicos o dispositivo será usado?** (ex.: dentro ou fora; parado ou em movimento; público ou privado; móvel ou imóvel; condições físicas e climáticas extremas ou específicas)
4. **Por quanto tempo espera-se que o dispositivo seja usado?** (ex.: algumas horas; vários anos; duas décadas)
5. **Que tipo de dependência em outros sistemas o dispositivo provavelmente terá?** (ex.: requer o uso de um determinado hub de IoT; usa serviços de terceiros baseados em nuvem para alguma funcionalidade)
6. **Como os invasores podem usar indevidamente e comprometer o dispositivo?** (ou seja, possíveis emparelhamentos de ameaças e vulnerabilidades, por exemplo, um modelo de ameaça que inclui considerações de conexões de rede que podem fornecer um atalho para a Internet para ser usado como um vetor de ataques contra outras redes ou dispositivos, como um ataque distribuído de negação de serviço)
7. **Que outros aspectos do uso do dispositivo podem ser relevantes para o risco de segurança cibernética do dispositivo?** (ex.: características operacionais do dispositivo que podem ter segurança, privacidade, ou outras implicações para os usuários)

3.2 Atividade 2: Investigar as necessidades e objetivos de cibersegurança do cliente

As necessidades e objetivos de cibersegurança serão principal mas não inteiramente impulsionadas pelos riscos de cibersegurança que os clientes enfrentam. Os fabricantes não conseguem entender completamente os riscos de todos os seus clientes, já que cada cliente, sistema e dispositivo IoT enfrenta riscos singulares com base em muitos fatores. Contudo, os fabricantes podem considerar os casos de uso esperados para seus dispositivos IoT e, em seguida, tornar seus dispositivos minimamente seguros para os clientes que os adquirem e usam de maneira consistente com os casos de uso. *Minimamente seguros* significa que os dispositivos possuem os recursos de cibersegurança que os clientes necessitam para mitigar alguns riscos comuns de segurança cibernética, o que os ajuda, pelo menos parcialmente, a cumprir os objetivos e atender às suas necessidades. Os clientes também exercem um papel importante na proteção dos seus dispositivos IoT e dos sistemas que os incorporam, incluindo o uso de meios técnicos, físicos e de procedimento. O grau em que um cliente exerce um papel nesse processo varia dependendo do caso, mas, para a maioria dos clientes e casos de uso, os recursos de segurança cibernética de dispositivo integrados aos dispositivos IoT geralmente tornam a mitigação de risco mais fácil e eficaz.

Os clientes usarão *meios* para alcançar suas necessidades e objetivos. *Meio* é definido como "um agente, ferramenta, dispositivo, medida, plano ou política para realizar ou promover um propósito [10].” Esta publicação refere-se aos meios técnicos e não técnicos para fins de cibersegurança, sejam eles realizados pelo próprio dispositivo IoT ou de outra maneira. O termo

introduzido na Seção 1, *recursos de cibersegurança do dispositivo*, refere-se a meios técnicos que estão sendo executados pelo próprio dispositivo IoT. Além desses meios técnicos, talvez haja outros meios, técnicos e não técnicos, ou serviços realizados e oferecidos pelo fabricante nos quais o cliente confia para fazer um planejamento e manter a segurança cibernética do dispositivo dentro dos seus sistemas e ambientes.

Conforme a Figure 2 demonstra, as conexões entre fabricantes e clientes no que concerne à segurança cibernética são importantes e devem ser levadas em consideração. Os clientes que compram e usam dispositivos IoT pretendem conectar esses dispositivos a sistemas e redes, incluindo a Internet. À medida que os clientes adotam esses dispositivos, eles procuram protegê-los para atender aos seus objetivos ou, possivelmente, esperam ter a segurança de acordo com as suas necessidades, que podem ou não ser articuladas diretamente pelo cliente. Os dispositivos IoT que suportam os recursos de cibersegurança desejados pelos clientes devem ser mais fáceis de proteger (ou essa é a expectativa), particularmente quando mecanismos que os clientes já implementaram estão sendo usados. Os fabricantes podem prever vários objetivos de cibersegurança dos clientes, especialmente aqueles baseados em orientações e requisitos de cibersegurança vigentes — por exemplo, clientes de um determinado setor podem ser obrigados, por regulamentação, a alterar todas as senhas padrão.

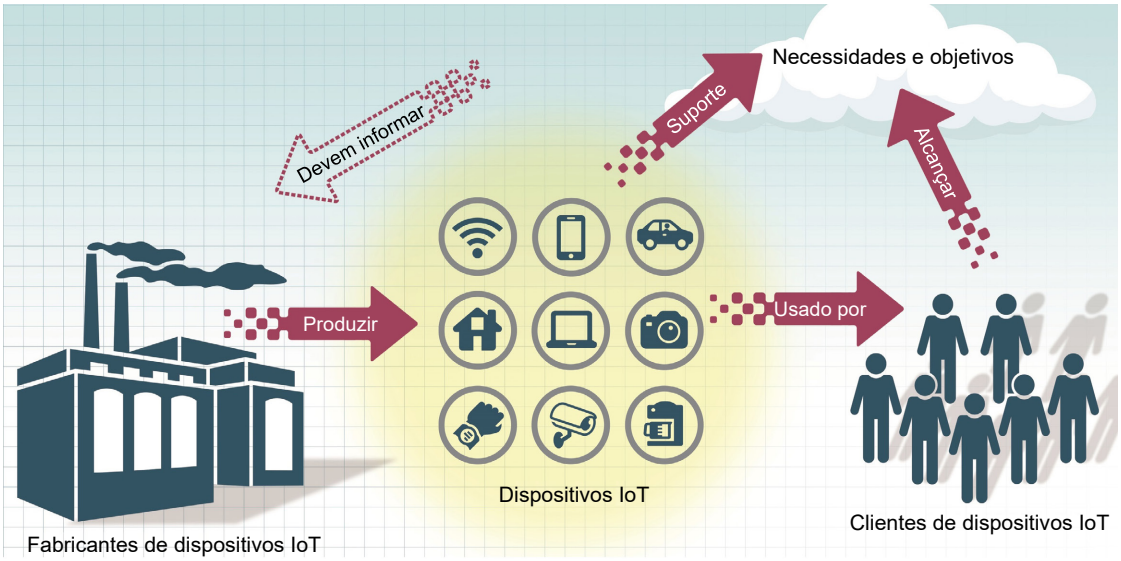

Figura 2: Conexões entre fabricantes de dispositivos IoT e clientes no tocante à cibersegurança

Os riscos de segurança cibernética para dispositivos IoT podem ser analisados em termos de duas mitigações de risco de alto nível. A primeira mitigação é proteger a cibersegurança do próprio dispositivo — para evitar que ele seja utilizado indevidamente para impactar negativamente o cliente, ou atacar outras organizações, ou não fornecer a funcionalidade esperada pelo cliente. A segunda é salvaguardar a confidencialidade, integridade e/ou disponibilidade de dados (incluindo informações pessoais) coletados, armazenados, processados ou transmitidos para o dispositivo IoT ou a partir dele.

Para coletar informações sobre as necessidades e objetivos dos clientes relacionados às salvaguardas de segurança cibernética do dispositivo e sua confidencialidade, integridade e

disponibilidade de dados, os fabricantes podem responder às seguintes perguntas para cada caso de uso esperado:

1. **Como o dispositivo IoT irá interagir com o mundo físico?** O impacto potencial de alguns dispositivos IoT que afetam o mundo físico, diretamente através da atuação ou indiretamente através da medição, pode resultar em requisitos operacionais relativos ao desempenho, confiabilidade, disponibilidade, resiliência e segurança que estejam em desacordo com as práticas comuns de cibersegurança para dispositivos convencionais de TI. Por exemplo, muitos dispositivos essenciais para a segurança devem continuar fornecendo algumas ou todas as funcionalidades no caso de um incidente de cibersegurança, problema de rede ou outra condição adversa.
2. **Como o dispositivo IoT deve ser acessado, gerenciado e monitorado por pessoas autorizadas, processos e outros dispositivos?** Alguns exemplos:
    - É importante considerar os métodos que provavelmente serão usados pelo cliente para gerenciar o dispositivo. Um dispositivo IoT pode oferecer suporte à integração com sistemas corporativos comuns (ex.: gestão de ativos, gerenciamento de vulnerabilidades, gerenciamento de log) para oferecer aos clientes que possuem esses sistemas, maior controle e visibilidade do dispositivo. No caso de um dispositivo IoT que será usado apenas no ambiente doméstico, esse recurso não seria relevante, pois o cliente espera uma maneira fácil de gerenciar o dispositivo, ou até mesmo quer que o fabricante execute todo o gerenciamento em seu nome (ex.: instalar patches automaticamente). Um dispositivo IoT usado por uma pequena empresa também pode ser gerenciado por terceiros em nome da empresa.
    - Tornar um dispositivo altamente configurável é geralmente mais indicado em ambientes de organização e menos indicado nas configurações de um cliente doméstico. É menos provável que um cliente doméstico entenda a importância das configurações granulares de segurança cibernética e, portanto, pode configurar um dispositivo incorretamente, enfraquecendo a segurança e aumentando a probabilidade de comprometimento. Também é improvável que alguns clientes domésticos queiram alterar as definições de configuração após a implantação inicial do dispositivo. No entanto, muitos clientes, inclusive clientes industriais, empresariais e domésticos, podem desejar algumas definições de configuração, como habilitar ou desabilitar serviços de sincronização de relógio para o dispositivo e escolher um servidor de tempo a ser usado na sincronização de relógio. A configuração do dispositivo pode ser totalmente omitida nos casos em que o dispositivo não precise ser provisionado ou customizado de alguma maneira durante ou após a implantação (ex.: não precisa ser conectado a uma rede sem fio, não precisa ser associado a um usuário específico).
    - Considere o nível de acessibilidade do dispositivo, seja logica ou fisicamente. Imagine uma máquina de venda de alimentos IoT em um local público, que é conectada à Internet para que os fornecedores possam rastrear o inventário e o status da máquina. Os usuários de máquinas de venda automática não seriam obrigados a usar a sua autenticação pessoal para inserir dinheiro e comprar um lanche. No entanto, a máquina de venda automática também seria altamente suscetível a ataques físicos.

- Considere se o dispositivo IoT deve ter uma interface de programação de aplicativos (API) aberta para oferecer suporte à integração, suporte geral ou desenvolvimento de terceiros. O acesso a uma API deve ser meticulosamente considerado e gerenciado como uma interface lógica, uma vez que pode oferecer acesso e funcionalidades significativas para entidades autorizadas.
- Considere permitir que os clientes desabilitem os recursos de segurança cibernética do dispositivo que possam impactar negativamente as operações. Um exemplo seria um recurso destinado a impedir ataques de força bruta contra senhas, como bloquear uma conta após muitas tentativas de autenticação com falha. Esse recurso pode causar inadvertidamente uma negação de serviço para a pessoa ou dispositivo que está tentando autenticar. Em ambientes críticos para a segurança, tais interrupções no acesso podem não ser aceitáveis devido ao perigo que causariam. Os clientes geralmente precisam de flexibilidade para configurar esses recursos ou desabilitá-los completamente.
- Considere a expectativa de vida útil do dispositivo e como isso pode afetar os recursos de segurança cibernética que são viabilizados durante esta expectativa. Alguns recursos de cibersegurança do dispositivo, como atualizações de software, exigirão desenvolvimento e esforços contínuos para fornecer os benefícios de cibersegurança intencionados. Além disso, alguns dispositivos IoT podem ter recursos não baseados em TI que podem e devem sobreviver à segurança cibernética ou vida útil da funcionalidade prevista para os componentes de TI do dispositivo.

3. **Quais são os requisitos conhecidos de segurança cibernética para o dispositivo IoT?** Os fabricantes podem identificar os requisitos conhecidos em seus casos de uso, como regulamentos de segurança cibernética específicos do setor, leis específicas do país, obrigações contratuais, expectativas do cliente ou maneiras convencionais para que possam estar atentos a esses requisitos durante a identificação dos recursos do dispositivo.
4. **Como o uso dos recursos de segurança cibernética pelo dispositivo IoT podem sofrer interferência pelas características operacionais ou ambientais do dispositivo?** Por exemplo, dispositivos que devem ser usados em largura de banda baixa ou redes não confiáveis talvez não possam usar certos recursos do dispositivo, como um mecanismo de atualização seguro. Dependendo da rede, o download de grandes atualizações pode saturar a conexão de rede, interrompendo outros usos, podendo demorar muito tempo para obter atualizações para o dispositivo. Os fabricantes podem considerar estratégias de atualização alternativas, como alterar seus processos para reduzir o tamanho das atualizações ou distribuir atualizações para administradores em conexões de rede de alta velocidade e fazer com que os administradores transfiram manualmente as atualizações para o dispositivo IoT (o que introduz riscos adicionais de cibersegurança da transmissão de malware por mídia removível que pode precisar ser mitigada).

   Usando outro exemplo, alguns dispositivos IoT, como equipamentos médicos conectados, podem fornecer funcionalidade crítica não baseada em TI para os clientes, e, portanto, os clientes possivelmente necessitarão dessas funções para continuar operando mesmo durante um estado de cibersegurança degradado ou quando a funcionalidade relacionada à TI (ex.: uma conexão com a Internet) ficar indisponível. O comportamento do

dispositivo em face à segurança cibernética degradada ou a uma redução do acesso à rede ou dados merece uma consideração cautelosa, pois isso é importante para que os fabricantes possam determinar como um dispositivo reage em condições adversas.

5. **Qual será a natureza dos dados do dispositivo IoT?** Existe uma grande variabilidade nos dados armazenados pelos dispositivos IoT; alguns dispositivos não armazenam nenhum dado, enquanto outros armazenam dados que podem causar danos significativos se acessados ou modificados por entidades não autorizadas. Compreender a natureza dos dados que se espera ter em um dispositivo no contexto dos clientes e casos de uso pode ajudar os fabricantes a identificar quais os recursos de cibersegurança do dispositivo são essenciais para proteger os dados, como criptografia de dados, autenticação de dispositivo e usuário, validação de dados, controle de acesso, e backup/restauração.
6. **Qual é o grau de confiança no dispositivo IoT que os clientes podem ter?** Os clientes podem esperar determinados recursos e implementações de cibersegurança do dispositivo que permitem garantias específicas de segurança cibernética do dispositivo e/ou dados. Por exemplo, em alguns contextos, o fabricante pode aumentar o grau de confiança de que os dados são protegidos, acrescentando a proteção de dados em uso pelo dispositivo. Esta medida vai além dos objetivos habituais de proteção de dados (ex.: proteger dados em repouso e em trânsito).
7. **Quais as complexidades que serão introduzidas pela interação do dispositivo IoT com outros dispositivos, sistemas e ambientes?** Por exemplo, a complexidade pode ser impulsionada por novos usos de IoT e de dispositivos IoT, novas combinações desses dispositivos entre si e dispositivos convencionais de TI, bem como o aumento das interconexões entre dispositivos e sistemas. Essas complexidades podem significar novas funcionalidades com implicações para a segurança humana ou privacidade, que serão conectadas por meio de tecnologias de rede a sistemas que não reduzem adequadamente esses riscos. Um dispositivo IoT que pode transmitir imagens dentro de uma casa, como um monitor inteligente para bebês, ou que pode alterar o ambiente de uma maneira potencialmente perigosa, como um forno inteligente, pode exigir salvaguardas normalmente não consideradas para dispositivos de TI convencionais. A IoT também pode apresentar complexidades relacionadas à escala, o que poderia dificultar o gerenciamento contínuo e o suporte de dispositivos.

Conforme a Figure 3 descreve conceitualmente, os fabricantes de dispositivos IoT podem usar uma variedade de fontes para coletar as informações de que precisam para responder a essas e a outras perguntas. Em alguns casos, os clientes potenciais e os casos de uso apontarão para leis, regulamentos ou orientações voluntárias em vigor para segurança cibernética e outros aspectos da operação do dispositivo. Por exemplo, os dispositivos IoT destinados a serem usados pelo governo federal seriam protegidos usando controles derivados de orientação de segurança cibernética de sistemas para agências federais (ex.: NIST SP 800-53 [6], Cybersecurity Framework [7]), que em alguns casos identifica ou implica recursos específicos de segurança cibernética de dispositivos que uma agência precisaria para oferecer suporte aos controles em seu sistema. Para alguns casos de uso, a orientação pode ir além dos riscos de cibersegurança, mas ainda terá implicações diretas ou indiretas para a segurança cibernética, como dispositivos no setor médico que precisam cumprir os regulamentos da Food and Drug Administration (FDA) e a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA). É possível que, para

atender às recomendações do FDA e aos requisitos da HIPAA, um dispositivo IoT possa precisar de proteção rigorosa de confidencialidade, integridade e/ou disponibilidade de dados, muito além do que está incluído em um dispositivo IoT comum. Ao compreender esses regulamentos no contexto dos dispositivos desses clientes e casos de uso esperados, os fabricantes podem determinar se e como melhor atender às necessidades e objetivos dos clientes no setor médico. Muitos setores industriais também chegarão a um consenso e/ou orientação voluntária que deve ser seguida por suas partes interessadas de várias formas, como estruturas, linhas de base e melhores práticas, dentre outras.

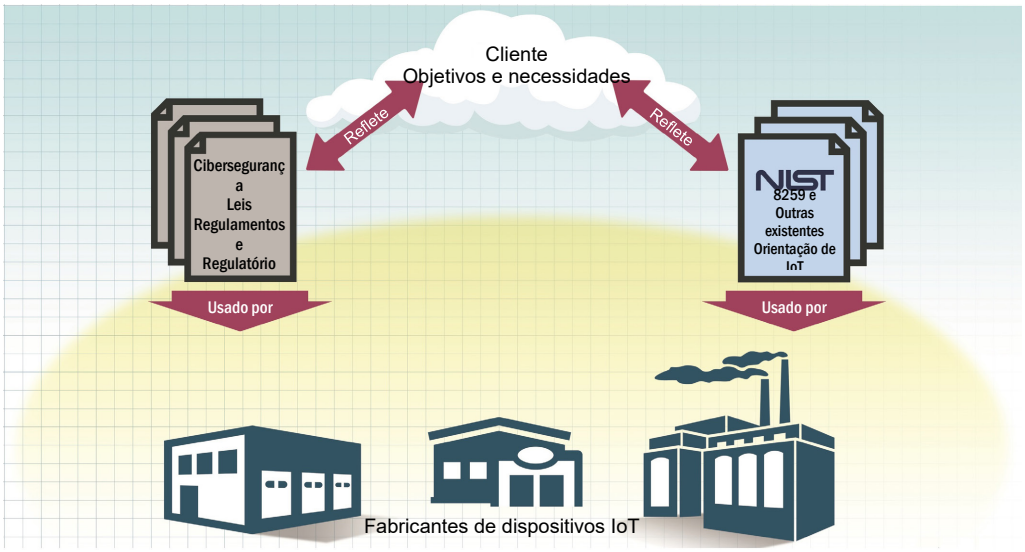

Figura 3: Necessidades e objetivos de cibersegurança do cliente refletidos e informados por muitos regulamentos e documentos de orientação aplicáveis

Para alguns clientes ou setores, essa orientação explícita por escrito pode não estar prontamente disponível ou utilizável (ex.: devido à alta variabilidade das necessidades e objetivos dos clientes dentro de determinado setor). Para dispositivos que serão usados por esses clientes, a averiguação de suas necessidades e objetivos pode exigir o uso de outras formas de informação, como a coleta de informações diretamente dos clientes ou a realização de pesquisas secundárias para melhor atender às suas necessidades e objetivos.

3.3 Atividade 3: Determinar como atender às necessidades e objetivos do cliente

Depois de pesquisar as necessidades e objetivos de cibersegurança do dispositivo IoT para clientes em potencial e casos de uso, os fabricantes podem determinar como atender a tais requisitos para ajudar os clientes a mitigar os riscos de segurança cibernética. Para cada necessidade ou objetivo de cibersegurança, o fabricante pode responder a seguinte pergunta: **qual o meio mais adequado (ou uma combinação de meios) para atender às necessidades e objetivos?**

- O dispositivo IoT pode proporcionar meios técnicos através de recursos próprios de cibersegurança (ex.: usando os recursos de cibersegurança do dispositivo integrados ao sistema operacional ou fazendo com que o software do dispositivo forneça recursos de cibersegurança do dispositivo).

- Outro dispositivo relacionado ao dispositivo IoT (ex.: um gateway ou hub IoT do fabricante ou de terceiros) pode fornecer os meios técnicos para os dispositivos IoT (ex.: agindo como um intermediário entre o dispositivo IoT e outras redes, ao mesmo tempo fornecendo funcionalidade de comando e controle para o dispositivo IoT).
- Outros sistemas e serviços que estejam agindo ou não em nome do fabricante podem fornecer os meios técnicos (ex.: um serviço baseado em nuvem que armazena dados de forma segura para cada dispositivo IoT, provedores de serviços de Internet e outros provedores de infraestrutura).
- Além do suporte por meios técnicos, os fabricantes e outras organizações e serviços também podem oferecer suporte por meios não técnicos quando estão agindo em nome do fabricante (ex.: comunicação de expectativa de vida e prazo de suporte, divulgação de planos de remediação de falhas).
- O cliente pode selecionar e implementar outros meios técnicos e não técnicos para mitigar os riscos de cibersegurança. (O cliente também pode optar por responder aos riscos de cibersegurança de outras maneiras, incluindo aceitá-lo ou transferi-lo.) Por exemplo, um dispositivo IoT pode ter sido instalado com o propósito de ser usado nas instalações do cliente, com controles rígidos de segurança física.

Observe que não há necessariamente uma equiparação "um a um" entre necessidades, objetivos e meios; por exemplo, vários meios técnicos podem ser necessários para atingir um objetivo, e um único meio técnico pode ajudar a atingir vários objetivos. Além disso, nem todas as necessidades e objetivos podem ou precisam ser atendidos usando apenas meios técnicos, sendo que alguns meios técnicos podem exigir outros meios não técnicos para a segurança inicial e contínua (ex.: saber quais os recursos de cibersegurança estão disponíveis em um dispositivo IoT, e qual a capacidade de reunir e aplicar atualizações de software).

Além de identificar os meios adequados para atender a cada necessidade e objetivo de cibersegurança, os fabricantes também podem responder a esta pergunta relacionada aos meios técnicos proporcionados pelo dispositivo IoT: **qual o nível de robustez deve ser implementado em cada meio técnico para que ele atenda efetivamente às necessidades ou objetivos de cibersegurança?** A robustez dos meios técnicos refere-se à força geral das implementações, sendo que ela se relaciona diretamente à confiança que um cliente pode ter em seu dispositivo IoT. Caso um dispositivo tenha sido criado para merecer maior confiança do cliente, particularmente para permanecer em um estado seguro e ficar fora do controle ou acesso de entidades não autorizadas, então é provável que os meios técnicos implementados no dispositivo, ou com o dispositivo, terão que ser mais robustos. Aqui estão alguns exemplos de possíveis considerações de robustez:

- Se ele precisa ser implementado em hardware e/ou software (ex.: um componente de hardware criptográfico emparelhado com software para usar a funcionalidade do hardware)
- Quais os dados que precisam ser protegidos e tipos de proteção em cada momento de necessidades de dados (ou seja, confidencialidade, integridade, disponibilidade) e qual deve ser a robustez desta proteção

- • Qual o nível de restrição que a identidade de uma entidade precisa ter para ser autenticada antes de se conceder acesso se for uma entidade humana (ex.: PIN, senha, frase de acesso, autenticação de dois fatores) ou um sistema/dispositivo (ex.: chaves de API, certificados)
- Se os dados recebidos ou inseridos no dispositivo precisam ser validados (ex.: para confirmar a legitimidade de uma atualização, para restringir a capacidade de dados malformados de contornar os controles de acesso)
- Com que rapidez as atualizações de software podem ser revertidas se ocorrer um problema (ex.: uma capacidade de reversão ou de anti-reversão)

Em última análise, os fabricantes podem agregar todos os meios técnicos identificados referentes às necessidades e objetivos para responder à seguinte pergunta: **quais serão os meios técnicos fornecidos pelo próprio dispositivo IoT, outros dispositivos relacionados ao dispositivo IoT, outros sistemas e serviços que atuam em nome do fabricante e do cliente, e quão robustos cada um desses meios deve ser?** O restante desta seção concentra-se na primeira parte da pergunta: quais serão os meios técnicos fornecidos pelo próprio dispositivo IoT - ou seja, recursos de cibersegurança do dispositivo?

A identificação dos recursos de cibersegurança do dispositivo que ele próprio precisa fornecer deve acontecer o mais cedo possível no processo de design para que tais recursos sejam levados em consideração no design do hardware e do software do dispositivo IoT. Para que os fabricantes tenham uma perspectiva inicial e possam identificar os recursos necessários de cibersegurança para os dispositivos IoT, sugerimos uma publicação complementar, NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [*Linha de base do núcleo para recursos de cibersegurança dos dispositivos IoT]* (*linha de base do núcleo)*,[4] que é um conjunto de recursos geralmente necessários para dispositivos, que dão suporte a controles comuns de cibersegurança que protegem os dispositivos, dados, sistemas e ecossistemas do cliente. A linha de base do núcleo foi derivada de abordagens comuns de gerenciamento de risco de cibersegurança, listadas no listadas no NISTIR 8259A.

A linha de base do núcleo é apenas um conjunto de recursos de segurança cibernética dos dispositivos que podem ser necessários em um dispositivo IoT, e os fabricantes devem consultar outras fontes para obter ou identificar recursos e implementações de segurança cibernética de dispositivos que sejam apropriados para clientes potenciais e casos de uso, conforme discutido na Seção 3.2. Os fabricantes podem seguir um processo para fazer uma lincagem da mitigação, necessidades e objetivos de cibersegurança com os recursos específicos de cibersegurança dos dispositivos. Este processo foi usado para criar a linha de base do núcleo conforme definida no NISTIR 8259A, onde as mitigações, necessidades e objetivos de cibersegurança de alto nível,

[4] O uso do termo "linha de base" nesta publicação não deve ser confundido com as linhas de base de controles de sistemas de baixo, moderado e alto impacto mencionadas na Publicação Especial NIST (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations [Controles de Segurança e Privacidade para Sistemas e Organizações Federais de Informação] [6] para ajudar os órgãos federais a cumprir suas obrigações no âmbito da Federal Information Security Modernization Act (FISMA) [Lei Federal de Modernização da Segurança da Informação] e outras regulamentações federais. No contexto dessas publicações, as linhas de base de controle de baixo, moderado e alto impacto se aplicam a um sistema de informação que pode incluir vários componentes, inclusive os dispositivos. Nesta publicação, a "linha de base" é usada no sentido genérico para se referir a um conjunto de requisitos ou recomendações fundamentais que se aplicariam a dispositivos IoT individuais destinados a serem usados como componentes dentro dos sistemas.

típicas para muitos clientes, foram usadas para determinar os recursos comuns de cibersegurança dos dispositivos. Os fabricantes podem implementar esses recursos em seus dispositivos IoT para ajudar o maior número possível de clientes a cumprir o número máximo de objetivos viável. Da mesma maneira, outras linhas de base para recursos de cibersegurança do dispositivo IoT já podem estar em uso através do NIST ou outras fontes, sendo que o design de algumas foi idealizado para atender às necessidades de grupos de clientes específicos, setores industriais, casos de uso, etc. Esses recursos, como a linha de base do núcleo, podem ajudar os fabricantes a identificar mais rapidamente os recursos de cibersegurança do dispositivo que sejam necessários no contexto em que o dispositivo IoT será usado. O NIST também pode lançar publicações adicionais, que fazem parte da série NISTIR 8259 que define mais recursos das linhas de base.

Visto que os recursos de cibersegurança do dispositivo serão decididos e moldados pelo cliente e de acordo com o contexto do caso de uso, diferentes dispositivos IoT precisarão de conjuntos diferentes de recursos de cibersegurança. O alto nível e a amplitude da linha de base do núcleo significam que será necessário traçar um perfil para dispositivos IoT específicos com base nas necessidades e objetivos singulares dentro dos contextos nos quais serão usados. O setor de dispositivos IoT pode orientar quanto aos objetivos e necessidades (ex.: médico, residencial, infraestrutura crítica), caso de uso (ex.: atuador de vida crítica, sensor de segurança crítica) ou outros fatores contextuais (ex.: necessidades específicas do cliente). Os recursos de cibersegurança do dispositivo que derivam da linha de base do núcleo podem ser traçados e desenvolvidos de várias maneiras. Recursos novos ou mais complexos que não foram identificados na linha de base do núcleo podem ser incluídos em um dispositivo. Os recursos de cibersegurança do dispositivo na linha de base do núcleo também podem ser expandidos e adaptados com elementos novos ou mais específicos, que melhor se alinham às necessidades e preferências dos clientes.

3.4 Atividade 4: Plano para suporte adequado às necessidades e objetivos do cliente

É importante que os fabricantes considerem como oferecer suporte às necessidades e objetivos dos clientes identificados, além da seleção de recursos de cibersegurança para dispositivos específicos e suas implementações de alto nível. Parte desse raciocínio é considerar como provisionar recursos de computação para oferecer suporte aos recursos de cibersegurança do dispositivo que atendam às necessidades e objetivos, e ações externas ao dispositivo que podem ser necessárias para haver suporte contínuo.

Os fabricantes podem ajudar a tornar seus dispositivos IoT mais seguros, provisionando adequadamente os recursos de hardware (ex.: processamento, memória, armazenamento, tecnologia de rede, energia), bem como recursos de software, para oferecer o suporte desejado aos recursos de cibersegurança do dispositivo. Por exemplo, a criptografia baseada em software é de processamento intensivo, e um dispositivo com processamento limitado e nenhuma criptografia baseada em hardware talvez não esteja apto a fornecer o que os clientes precisam. Outro exemplo é que alguns dispositivos não podem suportar o uso de um sistema operacional ou redes de Protocolo de Internet (IP), e um ou ambos podem ser necessários para suportar vários recursos de segurança cibernética dos dispositivos.

Durante a concepção do design e seleção dos recursos de hardware e software do dispositivo, os fabricantes podem responder às seguintes perguntas para os clientes potenciais e casos de uso, visando identificar necessidades de provisionamento e solução de possíveis problemas:

1. **1. Considerando o prazo de oferecimento de suporte e a vida útil do dispositivo, quais são os usos potenciais futuros que devem ser levados em consideração?** Por exemplo, se um dispositivo tem uma vida útil de 10 anos, pode ser necessário atualizar o algoritmo de criptografia ou o comprimento da chave que o dispositivo usa no decorrer desse tempo, e o novo algoritmo ou comprimento de chave pode exigir mais recursos de processamento do que os atuais. Deve-se considerar como o dispositivo poderá oferecer suporte às necessidades e objetivos de cibersegurança durante a vida útil do dispositivo, incluindo "provas futuras" que atestem os recursos de cibersegurança do dispositivo e suas implementações.
2. **Uma plataforma IoT já estabelecida pode ser usada em vez de adquirir e integrar componentes individuais de hardware e software?** Uma *plataforma IoT* é uma peça de hardware de dispositivo IoT e/ou software de suporte já instalado e configurado para uso de um fabricante como base de um novo dispositivo IoT. Uma plataforma IoT também pode oferecer serviços ou aplicativos de terceiros, ou um kit de desenvolvimento de software (SDK) para ajudar a acelerar o desenvolvimento de aplicativos IoT. Os fabricantes podem escolher uma plataforma IoT com recursos suficientes e adequadamente segura, em vez de criar um design de hardware, instalar e configurar um sistema operacional, criar novos serviços baseados em nuvem, escrever aplicativos de dispositivos IoT e aplicativos móveis, começando da estaca zero, além de executar outras tarefas que são propensas a erros e com maior probabilidade de introduzir novas vulnerabilidades ao dispositivo IoT, comparado a uma plataforma já estabelecida.
3. **Alguns recursos de segurança cibernética do dispositivo devem ser baseados em hardware?** Um exemplo é ter uma raiz de hardware de confiança que fornece armazenamento confiável para chaves criptográficas e permite realizar uma inicialização segura e confirmar a autenticidade do dispositivo. Além disso, os fabricantes devem ponderar se esses recursos baseados em hardware serão atualizáveis. Por exemplo, em alguns casos, os clientes precisarão de uma raiz de confiança do hardware imutável, nunca fazendo atualizações ou alterações nessa funcionalidade, porém, para outros clientes, tais limitações podem ser prejudiciais à segurança contínua.
4. **O hardware ou software (incluindo o sistema operacional) inclui recursos de dispositivo desnecessários com implicações de segurança cibernética? Se esse for o caso, eles podem ser desativados para evitar o uso indevido e exploração?** Por exemplo, um dispositivo pode ter interfaces locais na sua estrutura externa que são úteis ou essenciais para alguns ou futuros casos de uso esperados, mas o dispositivo pode ser implantado em áreas públicas por alguns clientes, onde essas interfaces estariam expostas a um possível ataque. As possíveis abordagens para esse problema podem ser, oferecer um invólucro resistente à violação para evitar o acesso físico às interfaces e uma opção de configuração que desativa logicamente as interfaces.

Os fabricantes devem considerar quais são práticas[5] de desenvolvimento seguro mais apropriadas para eles e os clientes, conforme planejam oferecer um suporte adequado às necessidades e objetivos do cliente. Os fabricantes podem usar respostas como as exemplificadas abaixo, com base nos clientes previstos e casos de uso para ajudar a identificar práticas adicionais de desenvolvimento seguro a serem adotadas com o propósito de melhorar a segurança cibernética dos dispositivos IoT:

1. **Como o código do dispositivo IoT é protegido contra acesso não autorizado e adulteração?** (por exemplo, repositório de código bem protegido, recursos de controle de versão, assinatura de código)

2. **Como os clientes podem verificar a integridade do hardware ou do software do dispositivo IoT?** (por exemplo, raiz de confiança de hardware, validação de assinatura de código, comparação de hash criptográfico)

3. **3. Que tipo de verificação é feita para confirmar se a segurança do software de terceiros usada no dispositivo IoT atende às necessidades dos clientes?** (por exemplo, verificar se há vulnerabilidades conhecidas que ainda não foram corrigidas, revisar ou analisar código legível por humanos, testar o código executável)

4. **Quais são as medidas utilizadas para minimizar as vulnerabilidades no software do dispositivo IoT que foi lançado?** (ex.: seguir práticas de codificação seguras, executar validação de entrada robusta, revisar e analisar código legível por humanos, testar o código executável, configurar o software para que ele tenha configurações seguras por padrão, verificar o código em bancos de dados de vulnerabilidades conhecidas)

5. **Quais são as medidas utilizadas para aceitar relatórios de possíveis vulnerabilidades de software dos dispositivos IoT e como responder a elas?** (ex.: programa de resposta a vulnerabilidades, monitoramento de banco de dados de vulnerabilidades, uso de serviço de inteligência de ameaças, desenvolvimento e distribuição de atualizações de software)

6. **Quais são os processos em vigor para avaliar e priorizar a remediação de todas as vulnerabilidades no software dos dispositivos IoT?** (ex.: estimar o esforço de remediação, estimar o impacto potencial da exploração, estimar os recursos do invasor necessários para transformar a vulnerabilidade em uma arma)

[5] Os fabricantes de dispositivos IoT interessados em obter mais informações sobre práticas seguras de desenvolvimento de software podem consultar o white paper do NIST Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) [Mitigando o Risco de Vulnerabilidades de Software Adotando uma Estrutura Segura de Desenvolvimento de Software] (SSDF) [11], que destaca práticas exclusivas para o desenvolvimento seguro de software. Cada uma dessas práticas é amplamente recomendada por publicações de desenvolvimento de software seguro, e o white paper fornece referências de quase 20 publicações sobre o tópico.

4 Atividades do fabricante que impactam a fase pós-mercado do dispositivo IoT

Os fabricantes de dispositivos IoT, em algum momento, colocarão no mercado os seus produtos para venda, isto é, os produtos estarão nas mãos dos clientes, o que dará início à fase pós-mercado. Mesmo nesta fase, quando os clientes estão cogitando possíveis compras de produtos e, depois que a venda é efetivada, os fabricantes continuam desempenhando um papel importante quanto ao oferecimento de suporte ao cliente para atender às necessidades e objetivos de cibersegurança dos dispositivos IoT. Por exemplo, os fabricantes podem ter que responder aos relatórios de vulnerabilidades e oferecer atualizações críticas. Essas atividades básicas de cibersegurança podem beneficiar os clientes e a capacidade que terão de proteger os dispositivos durante todo o ciclo de vida, o que influencia a decisão quando avaliam e adquirem dispositivos IoT disponíveis no mercado. Um aspecto que muitas vezes é negligenciado, tanto na fase de marketing quanto na fase pós-mercado, é a comunicação relacionada à segurança cibernética. Muitos clientes (ou os seus representantes) podem se beneficiar ao manterem uma comunicação constante com os fabricantes sobre os riscos de cibersegurança e o suporte às suas necessidades e objetivos quanto aos dispositivos IoT. Esta seção discute as medidas tomadas pelo fabricante com foco na segurança para o cliente, usando uma linguagem mais fácil para que os clientes possam entender e identificar como os dispositivos IoT são configurados para atender às suas necessidades e objetivos de cibersegurança, conforme exemplificado nas duas atividades abrangentes discutidas nesta seção.

As seções anteriores abordaram como os fabricantes podem identificar meios técnicos e não técnicos de cibersegurança, que os clientes e usuários de dispositivos IoT podem utilizar incluindo *recursos de segurança cibernética do dispositivo*. Esta seção tem como objetivo ajudar os fabricantes a definir como e o que devem comunicar sobre os riscos de cibersegurança referentes aos dispositivos IoT que atendam às necessidades dos clientes e usuários finais. Discutiremos alguns recursos adicionais de cibersegurança do dispositivo, como também, outras opções e serviços que o fabricante pode implementar, conforme apropriado, e que devem ser comunicados aos clientes.

Embora um planejamento para essas atividades não deva estar finalizado até que um dispositivo IoT esteja na fase pós-mercado (ex.: responder às perguntas feitas referentes a cada atividade) ele será melhor executado quando as informações necessárias estiverem disponíveis por meio de várias atividades pré-mercado, como as discutidas na Seção 3. Embora as atividades 1 a 4 ajudem a informar o planejamento e a execução das atividades apresentadas nesta seção, elas não são consideradas pré-requisitos. Isso permite que alguns ou todos os aspectos do planejamento das atividades 5 e 6 aconteçam paralelamente a outras atividades pré-mercado. As considerações mencionadas nessas atividades podem não se aplicar a todos os clientes ou fabricantes, porém, serão de grande valia para muitos deles.

4.1 Atividade 5: Definir abordagens para se comunicar com os clientes

A comunicação clara das informações de segurança cibernética pode exigir diferentes abordagens de comunicação para diferentes tipos de clientes, com base em suas expectativas e

recursos. Os fabricantes podem responder a perguntas como as mencionadas abaixo para ajudar a definir as abordagens de comunicação:

1. **Qual a terminologia que o cliente entenderá?** Por exemplo, um usuário doméstico provavelmente terá menos conhecimento técnico do que os pontos de contato em uma grande empresa (ex.: administradores de sistemas). Além disso, profissionais de TI e cibersegurança já podem estar familiarizados com maneiras convencionais de se referir a uma vulnerabilidade, de acordo com o número de Vulnerabilidades e Exposições Comuns (CVE).
2. **Quantas informações serão necessárias para o cliente?** Transmitir muitas informações aos clientes pode sobrecarregá-los e dificultar a localização das informações que realmente precisam. Não fornecer informações suficientes também não é uma abordagem recomendada, exceto nos casos em que revelar informações pode acarretar maiores implicações negativas — por exemplo, publicar detalhes técnicos de uma vulnerabilidade recém-descoberta antes que uma atualização esteja disponível para corrigir a vulnerabilidade.
3. **Como/onde as informações serão fornecidas?** As informações podem ser fornecidas em um ou mais locais lógicos e/ou físicos. Elas podem ser incluídas em manuais de usuário, termos de serviço e documentação de outros produtos, sites, e-mails e o próprio dispositivo IoT e seus aplicativos associados (ex.: aplicativos móveis). Será mais produtivo para os clientes se eles próprios conseguirem localizar as informações facilmente, sempre que necessário.
4. **Como a integridade das informações pode ser verificada?** Para alguns métodos de fornecimento de informações, como e-mails, os clientes podem preferir uma maneira de identificar se as informações são legítimas (ex.: que não seja uma tentativa de engenharia social).
5. **Os clientes terão que se comunicar com você como sendo o fabricante?** Por exemplo, os clientes podem buscar atualizações ou outros dados necessários para a manutenção dos seus dispositivos. Eles também podem detectar vulnerabilidades ou outros problemas que queiram relatar. A funcionalidade, usabilidade e eficácia dos canais de comunicação do cliente com o fabricante devem ser testados pelo fabricante para garantir que os clientes e outras partes (ex.: pesquisadores de segurança) possam efetivamente fazer uso dos canais.

4.2 Atividade 6: Decidir como e o que deve ser comunicado aos clientes

Existem várias opções que podem ser consideradas sobre qual o tipo de informação o fabricante deve comunicar aos clientes sobre determinado produto de IoT e qual o método de comunicação a ser usado. O restante desta seção contém exemplos de tópicos que os fabricantes podem optar por incluir em suas comunicações e ideias sobre como essas informações podem ser comunicadas em determinados casos.

4.2.1 Suposições relacionadas ao risco de cibersegurança

Para que os clientes possam melhor entender que os seus riscos podem ser diferentes das expectativas do fabricante, seria aconselhável que eles entendessem as suposições do fabricante

relacionadas à segurança cibernética quando na fase de design e desenvolvimento do dispositivo, como segue:

1. **Quais eram os clientes potenciais?** Por exemplo, alguns dispositivos IoT são criados para um setor ou tipo de cliente específico, o que pode impactar não apenas a implementação de determinados recursos de segurança cibernética, mas também o funcionamento do dispositivo.
2. **Como o dispositivo foi planejado para ser usado?** Por exemplo, alguns dispositivos IoT têm propósitos específicos em sistemas, o que pode induzir os clientes a considerar possibilidades de segurança cibernética. Além disso, presume-se que alguns dispositivos IoT devam ser usados em sistemas específicos, possivelmente criando dependências em cibersegurança com as quais os clientes devem estar familiarizados (ex.: um dispositivo requer conexão a um sistema de monitoramento para fins de cibersegurança).
3. **Em que tipo de ambiente o dispositivo seria usado?** Por exemplo, os clientes devem estar cientes da possibilidade de um dispositivo IoT não estar protegido caso esteja em um local público ou sem o uso de outro dispositivo que forneça alguns ou todos os recursos de cibersegurança em benefício do dispositivo IoT. A largura de banda e latência da rede, bem como outros fatores ambientais, também podem impactar as suposições feitas sobre como e quais os recursos que devem ser incorporados.
4. **Como as responsabilidades seriam compartilhadas entre o fabricante, o cliente e outros?** Por exemplo, alguns clientes podem estar interessados em saber se o uso total e a implementação dos recursos e tarefas relacionadas à cibersegurança do dispositivo são de responsabilidade de uma parte ou de várias partes (ex.: atualizações de software, configuração do dispositivo, proteção e destruição de dados e gerenciamento do dispositivo).

4.2.2 Expectativas de suporte e vida útil

A comunicação sobre o suporte oferecido e as expectativas de vida útil do dispositivo ajudam os clientes a planejar mitigações de risco de segurança cibernética em todo o ciclo de vida do dispositivo, o que pode ser um prazo mais curto comparado ao tempo em que o cliente deseja usar o dispositivo. Para determinar qual o tipo de informação comunicar aos clientes, os fabricantes podem responder às seguintes perguntas:

1. **Por quanto tempo você pretende oferecer suporte ao dispositivo?** Informar aos clientes por quanto tempo as atualizações e o suporte técnico estarão disponíveis pode ajudá-los a planejar o uso seguro e a manutenção dos dispositivos por um prazo de tempo apropriado.
2. **Qual foi o prazo estipulado para o fim da vida útil do dispositivo? Qual será o processo utilizado para o fim da vida útil?** Os clientes podem descontinuar o uso de um dispositivo quando o fabricante considerar o dispositivo como estando no final da vida útil. Esses clientes podem se beneficiar de uma notificação sobre o tempo restante (ex.: seis meses) antes do final da vida útil, para que possam planejar adequadamente.
3. **Quais as funcionalidades (se houver) que o dispositivo terá após o término do suporte e da vida útil?** Possivelmente, os clientes queiram saber se poderão continuar

usando o dispositivo no final da vida útil, mesmo se os serviços baseados em nuvem ou outras funções não estiverem mais disponíveis.

4. **Como os clientes podem relatar ao fabricante a suspeita de problemas com implicações de cibersegurança, como vulnerabilidades de software? Os relatórios serão aceitos após o término do suporte? Os relatórios serão aceitos após o término do ciclo de vida?** Exemplos de métodos para emissão de relatórios: números de telefone, endereços de e-mail e formulários da web.
5. **Como os clientes podem manter a segurança mesmo após o término do suporte técnico para o dispositivo (ex.: quando um fabricante ou uma organização terceirizada com uma função em cibersegurança encerra as atividades totalmente ou termina o suporte ao dispositivo)? Os arquivos ou dados essenciais serão disponibilizados em um fórum público para permitir que outras partes, e até mesmo os clientes, continuem oferecendo suporte ao dispositivo IoT?** Por exemplo, um fabricante que encerra as atividades pode disponibilizar a base de código do seu produto em um fórum de código aberto para permitir o desenvolvimento contínuo e o suporte da comunidade.

4.2.3 Composição e recursos do dispositivo

A comunicação de informações sobre o software, hardware, serviços, funções e tipos de dados do dispositivo ajuda os clientes a melhor entender e gerenciar a segurança cibernética dos seus dispositivos, especialmente se o cliente continuar desempenhando um papel fundamental no gerenciamento da segurança cibernética do dispositivo. Para determinar quais são as informações importantes para comunicar aos clientes, os fabricantes podem responder às seguintes perguntas:

1. **Quais as informações que os clientes precisam ter sobre aspectos gerais relacionados à segurança cibernética do dispositivo, englobando a instalação, configuração (incluindo endurecimento do sistema), uso, gerenciamento, manutenção e descarte?** Os exemplos incluem como o dispositivo pode se conectar seguramente a um sistema ou rede, quais as opções e tipos de configuração que podem impactar a segurança cibernética, e quais são as maneiras de usar o dispositivo que são consideradas inseguras.
2. **Qual é o efeito potencial no dispositivo se a configuração de cibersegurança for mais restritiva do que o padrão?** Por exemplo, alguns dispositivos podem perder a funcionalidades à medida que suas configurações de cibersegurança se tornam mais rígidas.
3. **Quais as informações de inventário os clientes precisam saber em relação ao software interno do dispositivo, como versões, status de patch e vulnerabilidades conhecidas? Os clientes precisam ter acesso ao estoque atual mediante demanda?** Por exemplo, alguns clientes podem querer estar cientes das vulnerabilidades conhecidas para que possam abordá-las por outros meios, enquanto outros clientes podem querer saber o status atual do patch de software.
4. **Quais as informações que os clientes precisam saber sobre as fontes do software, hardware e serviços do dispositivo?** Exemplos de fontes incluem o desenvolvedor do

software do dispositivo IoT, o fabricante do processador e o provedor de um serviço baseado em nuvem usado pelo dispositivo.[6]

5. **Quais as informações que os clientes precisam saber sobre as características operacionais do dispositivo para que possam protegê-lo adequadamente? Como essas informações devem ser disponibilizadas?** Por exemplo, alguns clientes podem ser melhor atendidos colocando as informações em um site da Web, enquanto outros podem fazer o melhor uso das informações por meio de um protocolo padronizado de máquina a máquina. Em alguns casos, como para sinalização de intenção do dispositivo, essas informações podem ser melhor fornecidas através do próprio dispositivo.
6. **Quais funções o dispositivo pode executar?** Isso inclui não apenas os recursos de segurança cibernética do dispositivo, mas também qualquer outra função que possa ter implicações de cibersegurança - por exemplo, a transmissão de dados para um sistema remoto ou o uso de um microfone e câmera para capturar áudio e vídeo.
7. **Que tipos de dados o dispositivo pode coletar? Quais são as identidades de todas as partes (incluindo o fabricante) que podem acessar esses dados?** Por exemplo, alguns clientes talvez precisem saber se as informações de localização ou comandos de voz coletados pelo dispositivo podem ser armazenadas em uma nuvem e acessados para outros fins, possivelmente por outras partes (por exemplo, para agregação ou análise).
8. **Quais são as identidades de todas as partes (incluindo o fabricante) que têm acesso ou qualquer grau de controle sobre o dispositivo?** Por exemplo, um terceiro que fornece suporte técnico em nome do fabricante pode ter a possibilidade de atualizar remotamente o software e a configuração do dispositivo.

4.2.4 Atualizações de software

Os fabricantes que comunicam informações sobre atualizações de software ajudam os clientes a planejar mitigações de risco e manter a cibersegurança dos seus dispositivos, particularmente em resposta a ameaças emergentes. Para determinar quais as informações de atualização que são importantes para comunicar aos clientes, os fabricantes podem responder às seguintes perguntas:

1. **As atualizações serão disponibilizadas? Em caso afirmativo, quando serão lançadas?** Por exemplo, saber se as atualizações serão fornecidas de acordo com um cronograma definido ou se serão feitas esporadicamente ajudará os clientes a planejar quando deverão implementá-las
2. **Em quais circunstâncias as atualizações serão lançadas?** Os exemplos incluem o controle da execução de software defeituoso e a correção de uma vulnerabilidade anteriormente desconhecida em um protocolo padrão.
3. **Como as atualizações serão disponibilizadas ou entregues? Haverá notificações quando as atualizações estiverem disponíveis ou aplicadas?** Por exemplo, os clientes podem melhor planejar a aplicação de atualizações se souberem que devem ser baixadas

[6] Técnicas como, por exemplo, usar uma lista de materiais de software (SBOM) podem ser consideradas uma forma de comunicar tais informações aos clientes, e outras semelhantes, de maneira consistente e eficaz. Mais informações sobre o SBOM estão disponíveis na [National Telecommunications and Information Administration] Administração Nacional de Telecomunicações e Informações (https://www.ntia.gov/SBOM).

de um portal específico e aplicadas ao dispositivo. Os clientes também podem se beneficiar se forem notificados de que uma atualização deve ser feita ou foi aplicada, mesmo nos casos em que a entrega e a aplicação da atualização de software forem feitas automaticamente, não exigindo nenhuma ação do cliente ou do usuário.

4. **Qual a entidade (ex.: cliente, fabricante, terceiro) é responsável por realizar as atualizações? Ou o cliente pode designar qual entidade será responsável (ex.: automaticamente aplicada pelo fabricante)?** Por exemplo, alguns clientes podem se beneficiar sabendo que certas atualizações estarão disponíveis via terceiros e as outras atualizações serão fornecidas pelo fabricante. Alguns clientes também podem se beneficiar ao serem informados sobre suas funções, responsabilidades e opções em relação às atualizações.
5. **Como os clientes podem verificar e autenticar as atualizações?** Os exemplos são: comparação criptográfica de hash, validação de assinatura de código, e confiança no software fornecido pelo fabricante que executa automaticamente a verificação de atualização e autenticação.
6. **Quais as informações que devem ser comunicadas juntamente com cada atualização individual?** Os exemplos são: a natureza da atualização (isto é, correções de erros, recursos alterados ou novos) e qualquer efeito que a instalação da atualização possa ter nas configurações existentes de um cliente.

4.2.5 Opções de desativação do dispositivo

Os fabricantes que comunicam informações sobre as opções de desativação do dispositivo (ex.: a capacidade de "descomissionar" o dispositivo, possivelmente por meio de uma redefinição de dados ou tornando o dispositivo inoperante) ajuda os clientes a planejar esse processo com segurança. Para determinar quais as informações de atualização que são importantes para comunicar aos clientes, os fabricantes podem responder às seguintes perguntas:

1. **Os clientes desejarão transferir a propriedade dos seus dispositivos para outra parte? Se esse for o caso, o que os clientes precisam fazer para que os dados e configuração de usuário do dispositivo e sistemas associados (ex.: serviços baseados em nuvem usados pelo dispositivo) fiquem inacessíveis pela parte que assume a propriedade?** Por exemplo, um cliente decide vender um imóvel que contém dispositivos inteligentes de automação de edifícios, mas gostaria de ter uma garantia de que todos os dados foram removidos dos dispositivos antes que o comprador tenha acesso.
2. **Os clientes desejarão tornar os seus dispositivos inoperantes? Caso afirmativo, como os clientes podem fazer isso?** Por exemplo, alguns dispositivos IoT podem se tornar inoperantes por meio de meios lógicos (ex.: conforme executado através de um aplicativo móvel), enquanto outros usam meios físicos (ex.: um botão no dispositivo).

4.2.6 Meios técnicos e não técnicos

Comunicar informações sobre os recursos de cibersegurança do dispositivo (meios técnicos dentro do dispositivo) ajuda os clientes na gestão de risco. As informações podem ser sobre os meios técnicos fornecidos por um dispositivo relacionado, serviço ou sistema do fabricante, ou meios não técnicos fornecidos pelo fabricante e/ou terceiros, sendo que os clientes podem utilizar os meios não-técnicos por si próprios, o que os ajuda a melhor gerenciar os riscos do dispositivo. Para determinar quais são as informações importantes sobre os recursos de cibersegurança do dispositivo a serem transmitidas aos clientes, os fabricantes podem responder às seguintes perguntas:

1. **Quais os meios técnicos que serão fornecidos**
    a. **pelo próprio dispositivo (recursos de cibersegurança do dispositivo)?** Os exemplos incluem criptografia usada pelo dispositivo para proteção de dados, a presença de um identificador físico no dispositivo e mecanismos de autenticação e autorização que o dispositivo usa para limitar o acesso às suas interfaces de rede.
    b. **por um dispositivo relacionado?** Por exemplo, alguns meios técnicos podem ser fornecidos ou suportados por um hub de IoT ou dispositivo móvel ao qual o dispositivo IoT está associado.
    c. **por um serviço ou sistema do fabricante?** Um exemplo disso são os meios técnicos fornecidos por um servidor de Internet ou serviço hospedado em nuvem.
2. **Quais os meios não técnicos que podem ser fornecidos pelo fabricante ou outras organizações e serviços agindo em nome do fabricante?** Os exemplos incluem muitos dos conceitos discutidos ao longo desta seção, como expectativa de vida, planos de atualização de software e opções de desativação. Além dos exemplos discutidos nesta seção, existem outros meios não técnicos (ex.: maneira em que uma falha ou vulnerabilidade pode ser relatada) de que os clientes se beneficiariam em saber e compreender.
3. **Quais os meios técnicos e não técnicos que o cliente deve optar por obter?** Os exemplos seriam o uso de controles de segurança baseados em rede (um firewall) para evitar o acesso direto ao dispositivo pela Internet e a realização de auditorias da implementação e das configurações dos dispositivos para garantir que os requisitos de compliance estão sendo atendidos.
4. **Como os meios técnicos e não técnicos podem afetar os riscos de cibersegurança?** Por exemplo, a implementação adequada da proteção de dados pode ajudar a mitigar os riscos de confidencialidade, mas também pode reduzir a disponibilidade (ex.: se os dados não podem ser descriptografados ou são descriptografados lentamente), o que pode aumentar os riscos de disponibilidade.

5 Conclusão

Esta publicação discute seis atividades relacionadas à segurança cibernética para fabricantes de dispositivos IoT e oferece exemplos de perguntas que os fabricantes podem responder referentes a cada atividade. Os fabricantes que optarem por realizar uma ou mais dessas atividades básicas de cibersegurança devem determinar a aplicabilidade das perguntas que servem de exemplo e identificar outras perguntas que possam ajudar a entender as necessidades e objetivos de cibersegurança dos clientes, incluindo os recursos de cibersegurança do dispositivo que os clientes esperam ter. As questões destacadas para cada atividade são consideradas uma perspectiva inicial e não definem inteiramente cada atividade. Além disso, o processo descrito nesta publicação não implica que a função dos fabricantes se limite a fornecer recursos que exigem uma reação dos clientes, mas o intuito é fazer que os fabricantes compreendam as necessidades e objetivos dos clientes no contexto do dispositivo IoT, que pode exigir recursos automatizados e/ou medidas adicionais não técnicas de oferecimento de suporte. Para alguns clientes e casos de uso, onde for possível e adequado, a responsabilidade limitada pela segurança cibernética pode levar a melhores resultados de segurança cibernética para os ecossistemas do que se a responsabilidade fosse total e exclusivamente do cliente.

Referências

[1] Simmon E (a ser lançado) [A Model for the Internet of Things (IoT)]. Um Modelo para a Internet das Coisas (IoT). (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD).

[2] Ordem Executiva nº 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [*Fortalecimento da Cibersegurança de Redes Federais e Infraestrutura Crítica]*, DCPD-201700327, 11 de maio de 2017. https://www.govinfo.gov/app/details/DCPD-201700327

[3] Departamento de Comércio (2018) A Road Map Toward Resilience Against Botnets [Um Roteiro para a Resiliência Contra Botnets]. (Departamento de Comércio, Washington, DC). https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf

[4] Fagan M, Megas KN, Scarfone K, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline [Linha de base do núcleo para recursos de cibersegurança dos dispositivos IoT]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD), NIST Interagência ou Relatório Interno (IR) 8259A. https://doi.org/10.6028/NIST.IR.8259A

[5] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations [Iniciativa de Transformação da Força Tarefa Conjunta (2013) Segurança e Controles de Privacidade para Organizações e Sistemas de Informação Federais]. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Publicação Especial do NIST (SP) 800-53, Rev. 4, inclui atualizações a partir de 22 de janeiro de 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[6] Instituto Nacional de Padrões e Tecnologia (2018) Framework for Improving Critical Infrastructure Cybersecurity [Guia para Melhorar a Segurança Cibernética da Infraestrutura Crítica], Versão 1.1 (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[7] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, Gabel O'Rourke D, Scarfone K (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks [Considerações para gerenciar riscos de cibersegurança e privacidade na Internet das Coisas (IoT)]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD), NIST Interagência ou Relatório Interno (IR) 8228. https://doi.org/10.6028/NIST.IR.8228

[8] Stouffer K, Pillitteri V, Lightman S, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security [Guia (de 2015) para Segurança de Sistemas de Controle Industrial (ICS)]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD), Publicação Especial do NIST (SP) 800-82, Rev 2. https://doi.org/10.6028/NIST.SP.800-82r2

[9] Grupo de Trabalho Público de Sistemas Ciber-Físicos (2017) Framework for Cyber-Physical Systems: [Estrutura para sistemas ciberfísicos]: Volume 1, Visão Geral, Versão 1.0. (Instituto Nacional de Normas e Tecnologia) Publicação Especial do NIST (SP) 1500-201. https://doi.org/10.6028/NIST.SP.1500-201

[10] Merriam-Webster (2017) Texto Integral do Terceiro Novo Dicionário Internacional de Webster. (Merriam-Webster, Springfield, MA).

[11] Dodson D, Souppaya M, Scarfone K (2019) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) [Mitigando o risco de vulnerabilidades de software adotando uma estrutura segura de desenvolvimento de software (SSDF)]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD), NIST White Paper sobre Cibersegurança. https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-software-vulnerabilities-with-ssdf/final

Appendix A—Siglas e Abreviações

As siglas e abreviações selecionadas e usadas neste documento são definidas abaixo:

API	Application Programming Interface (Interface de programação de aplicativos)
CVE	Common Vulnerabilities and Exposures (Vulnerabilidades e Exposições Comuns)
DDoS	Distributed Denial of Service (Negação de serviço distribuído)
FISMA	Federal Information Security Modernization Act (Lei Federal de Modernização da Segurança da Informação)
FOIA	Freedom of Information Act (Lei de Liberdade de Informação)
ICS	Sistema de Controle Industrial
IoT	Internet das Coisas
IP	Internet Protocol (Protocolo da Internet)
IR	Relatório Interno
TI	Tecnologia da Informação
ITL	Laboratório de Tecnologia da Informação
LTE	Evolução a longo prazo
MAC	Controle de acesso à mídia
NIST	Instituto Nacional de Normas e Tecnologia
PII	Personally Identifiable Information (Informações Pessoalmente Identificáveis)
ROM	Read-Only Memory (Memória somente de leitura)
SBOM	Lista de Materiais de Software
SDK	Kit de Desenvolvimento de Software
SP	Publicação especial
SSDF	Secure Software Development Framework (Estrutura de desenvolvimento de software seguro)
USB	Universal Serial Bus (Porta serial universal)
UWB	Ultra-Wideband (banda ultra larga)
Wi-Fi	Fidelidade sem fio

Appendix B—Glossário

Os termos selecionados e utilizados neste documento são definidos abaixo.

Atuador	Uma porção de um dispositivo IoT que consegue mudar algo no mundo físico [7].
Linha de base do núcleo	Um conjunto de recursos técnicos de dispositivos necessários para dar suporte a controles comuns de segurança cibernética que protegem os dispositivos do cliente e seus dados, sistemas e ecossistemas.
Linha de base do núcleo para recursos de cibersegurança do dispositivo	Veja *linha de base do núcleo*.
Recursos de cibersegurança do dispositivo	Um recurso ou função de segurança cibernética fornecida por um dispositivo IoT através dos seus próprios meios técnicos (ou seja, hardware e software do dispositivo).
Plataforma IoT	Uma peça de hardware do dispositivo IoT com software de suporte já instalado e configurado para uso do fabricante como base para um novo dispositivo IoT. Uma plataforma IoT também pode oferecer serviços ou aplicativos de terceiros ou um kit de desenvolvimento de software para ajudar a agilizar o desenvolvimento de aplicativos IoT.
Meio	"Um agente, ferramenta, dispositivo, medida, plano ou política para realizar ou promover um propósito [10]."
Dispositivo IoT minimamente seguro	Um dispositivo IoT que possui os recursos de cibersegurança do dispositivo (ou seja, hardware e software) que os clientes podem precisar implementar e utilizar para mitigar alguns riscos comuns de segurança cibernética.
Interface de rede	Uma interface que conecta um dispositivo IoT a uma rede (ex.: Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB]).
Sensor	Uma parte de um dispositivo IoT que fornece uma observação de determinado aspecto do mundo físico na forma de dados de medição [7].
Transdutor	Uma parte de um dispositivo IoT que interage diretamente com uma entidade física de interesse. Os dois tipos de transdutores são sensores e atuadores [7].