O IoT Precisa de Melhor Segurança

A Internet das Coisas (IoT) é um ecossistema de coisas conectadas (dispositivos estacionários ou móveis). Um relatório de 2016 da *Business Insider* afirmou que haverá 34 bilhões de dispositivos conectados à Internet até 2020, frente aos 10 bilhões em 2015. Além disso, dispositivos IoT serão responsáveis por 24 bilhões deles, enquanto dispositivos de computação tradicionais (ex.: smartphones, tablets, smartwatches) compreenderão 10 bilhões. E, quase 6 trilhões de dólares serão gastos em soluções IoT durante os próximos cinco anos.[1]

Por Que Precisamos de Segurança em IoT?

A indústria está mudando rapidamente e novos casos de uso de IoT estão amadurecendo. Mais e mais funcionalidades estão sendo adicionadas aos sistemas IoT para vantagens e benefícios funcionais pioneiros do mercado, enquanto a segurança dos dispositivos do sistema IoT é muitas vezes ignorada durante o projeto. Isso é evidente em alguns casos recentes de ataques de hackers:

- A Food and Drug Administration dos EUA emitiu parecer de segurança para aparelhos cardíacos por causa de uma ameaça hacker e o Hospital de Pesquisa Infantil St. Jude corrigiu dispositivos IoT médicos vulneráveis.[2]
- Hackers demonstraram um ataque sem fio no automóvel Modelo Tesla S.[3]
- Pesquisadores hackearam Smart TVs Vizio para acessar uma rede doméstica.[4]

Outras origens de oportunidades de segurança perdidas ocorrem durante a configuração de instalação e de pós-instalação de IoT. Uma pesquisa de segurança em IoT da ForeScout apontou que "Os entrevistados, que inicialmente pensavam que não tinham dispositivos IoT em suas redes, na verdade tinham oito tipos de dispositivos IoT (quando solicitados a escolher de uma lista de dispositivos) e apenas 44% tinham uma política de segurança conhecida para IoT". [5] Apenas 30% estavam seguros que realmente sabem o que são dispositivos IoT em sua rede.[6]
Estes ataques e as implicações dos resultados da pesquisa da ForeScout indicam que a segurança IoT precisa ser implementada holisticamente. Isso requer uma compreensão da arquitetura de IoT.

Arquitetura de IoT

A Estrutura Zachman[7] responde por que, como, o quê, quem, onde e quando às perguntas relativas a "IoT. A pergunta porquê relativa à segurança de IoT já foi abordada aqui. As respostas para como e o que são explicadas nas quatro "camadas da arquitetura. **Figura 1** descreve a arquitetura de segurança de "IoT explicada através das "perguntas a serem respondidas durante a abordagem da Estrutura de Zachman.

FIGURA 1—Estrutura Zachman Arquitetura Contextual para Segurança de IoT

Perguntas	Segurança de IoT
Por Que?	Exemplos de violações de segurança, modelagem de ameaças
Como?	Configuração e integração do dispositivo, padrões, processos
O Quê?	Lista de componentes e seus relacionamentos
Quem?	Usuário, administrador, fabricante, organismos industriais
Onde?	Em cada camada e componente na arquitetura
Quando?	Design, configuração/implementação e operações

Fonte: H. Patel. Reimpresso com permissão.

É preciso existir uma compreensão conceitual de alto nível de IoT para entender os requisitos de segurança de IoT. As informações fluem da camada da margem (ou seja, dispositivos, conjuntos/máquinas de IoT) para a camada de dados para a camada de inteligência

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Hemant Patel, CISM, ITIL, PMP, TOGAF
É conselheiro principal da Computer Sciences Corporation, SC, como parte da equipe da Diretoria de Tecnologia dos Estados Unidos. Sua experiência inclui arquitetura corporativa de TI, segurança de informações, planejamento de portfólio, big data, web e comércio eletrônico, análise, planejamento de recursos corporativos e sistemas de gerenciamento de relacionamento com clientes. Sua experiência global inclui trabalho nas indústrias de defesa, produção, saúde, serviços públicos, bancos e seguros. Ele pode ser contatado nos e-mails: hpatel63@csc.com or mr.hemant.patel@hotmail.com.

Você está gostando deste artigo?

- Leia *Internet of Things: Considerações sobre Risco e Valor.* *www.isaca.org/internet-of-things*
- **Obtenha mais informações, discuta e colabore sobre a segurança cibernética no Centro de Conhecimento.** *www.isaca.org/information-security-policies-and-procedures*

empresarial (BI) para a camada de operações e de estratégia (OpS), como mostrado na **Figura 2**. Uma rede local ou uma rede remota conecta os dispositivos e camadas. Muitas vezes, muitos dispositivos são agrupados para oferecer suporte a um conjunto de componentes ou uma máquina. A comunicação entre dispositivos pode ou não estar presente em um conjunto ou uma máquina. Dispositivos e conjuntos se conectam a um hub ou um gateway para encapsular recursos exclusivos do dispositivo e para melhor padronização e gerenciamento.

Uma abordagem de segurança holística inclui segurança para cada camada e segurança de comunicações entre as camadas. Camadas diferentes da camada de borda podem ser hospedadas localmente ou em nuvem. É importante compreender os requisitos de segurança em cada uma das camadas.

Segurança da Camada de Borda

A segurança de IoT deve ser parte de um tema mais amplo da segurança da informação. Os dispositivos / sensores da camada de borda produzem dados que são processados por componentes em camadas superiores da arquitetura de IoT. O volume de dados é muito maior do que, e diferentemente, do volume de dados produzido pela atividade do usuário de Internet.

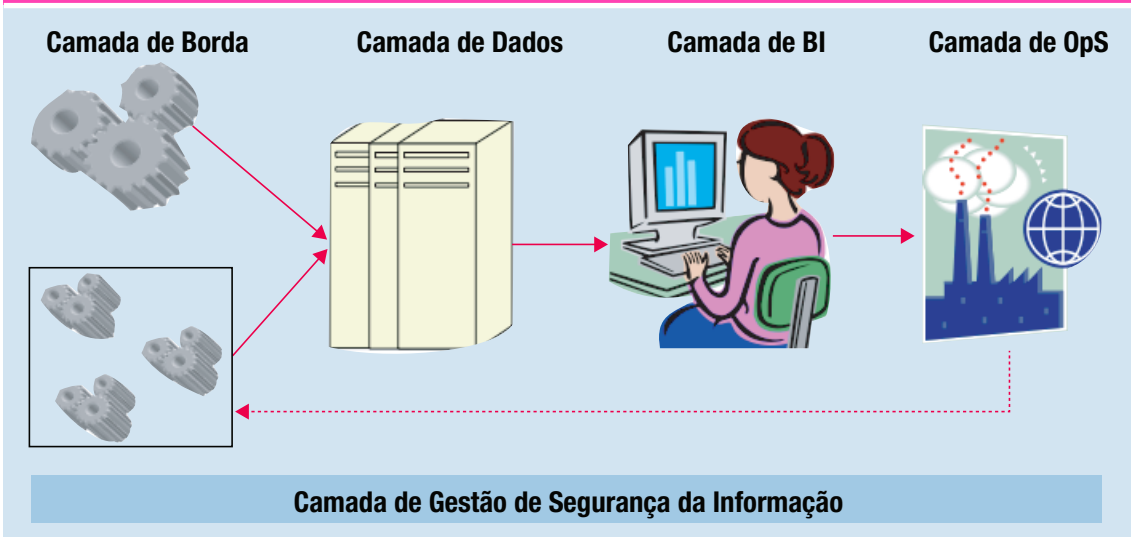
Há uma concorrência significativa em segurança baseada em dispositivos e espaço de software de gerenciamento de hub/gateway de IoT, e há uma infinidade de padrões. Organizações como a Microsoft, IBM e Allegro fizeram um bom trabalho ao empacotar a segurança baseada em dispositivos em Interfaces de programação de aplicativos (APIs) e ferramentas de nível mais elevado. Os blocos básicos de construção da arquitetura de segurança da camada de borda são mostrados na**figura 3**. O hub ou o gateway oferece suporte aos componentes de administração de segurança, gerenciamento de armazenamento e comunicação relacionados à segurança de IoT. Os dispositivos podem se interconectar ou se comunicar com hubs, e esse software de comunicação precisa de um menor requisito de espaço com recursos de enfileiramento. O Protocolo de Controle de Transmissão (TCP), baseado em soquete, comunicação

> **"Uma abordagem de segurança holística inclui segurança para cada camada e segurança de comunicações entre as camadas."**

ponto-a-ponto foi usado anteriormente, que foi depois seguido por melhores protocolos, incluindo:

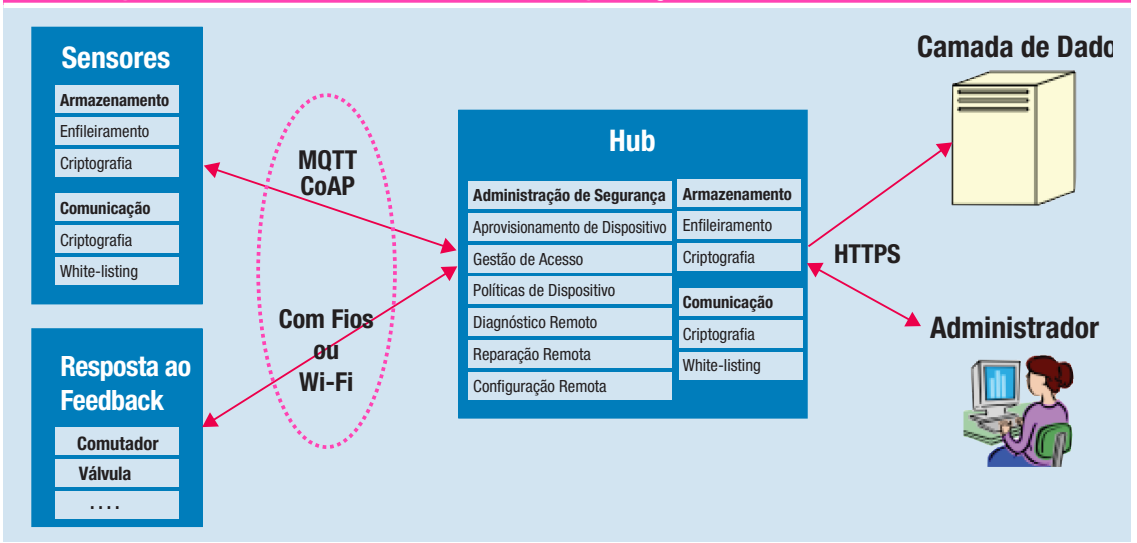
- **Transporte de Enfileiramento de Mensagens Telemetria (MQTT)**—Um protocolo baseado em TCP que suporta autenticação de dispositivo, criptografia, enfileiramento e recursos de publicação de assinatura de Camada de Soquete Seguro (SSL)/Segurança de Camada de Transporte (TLS)

FIGURA 2—Arquitetura Conceitual de IoT



Fonte: H. Patel. Reimpresso com permissão.

Figura 3—Arquitetura Conceitual de Segurança da Camada de Borda de IoT



Fonte: H. Patel. Reimpresso com permissão.

- **Protocolo de Aplicação Restrita (CoAP)** - Um transporte baseado em Protocolo de Datagramas de Usuário (UDP), oferece suporte a microdispositivos e tem um requisito de espaço muito menor que o HTTP. Ele oferece suporte ao Padrão Avançado de Criptografia (AES).[8]

Uma rede local sem fios (WLAN) é utilizada em muitas áreas com segurança WPA2. A segurança Wi-Fi é mais comumente hackeada devido à configuração de segurança inadequada e má escolha de senhas. Um gateway pode se conectar com vários hubs e fornecer protocolos de transferência de dados de maior nível, como o HTTPS, que oferece suporte à criptografia TLS e sistema de mensagens Transferência Representacional de Estado (REST)-Protocolo Simples de Acesso a Objetos (SOAP).

Os fornecedores de dispositivos e de hubs precisam oferecer suporte a protocolos e gerenciamento de segurança, conforme aqui descrito, e esse suporte pode se complicar devido a autenticação de múltiplos protocolos e de suporte através dos protocolos.

Outro problema a ser monitorado é o mau funcionamento do dispositivo IoT. Um mau funcionamento pode ocorrer devido a uma violação de segurança ou por outras razões. Um mau funcionamento pode resultar em um dispositivo tentar acessar os dados e, sem uma configuração adequada limitando o número de tentativas, pode haver um número infinito de tentativas. Quando cada tentativa envia uma mensagem de erro ao hub, o hub pode acabar recebendo infinitas mensagens de erro (semelhante a um ataque de negação de serviço distribuído [DDoS]) e o hub de IoT pode tornar-se inoperacional devido a carga excessiva, afetando assim a disponibilidade do hub.

Um mau funcionamento pode impedir que um dispositivo IoT gere dados. Isso faz com que o hub não receba nenhum dado, o que afeta a integridade do hub. Assim, um mau funcionamento do dispositivo pode afetar a disponibilidade e a integridade (qualidades básicas da segurança da informação) da segurança de IoT.

Segurança da Camada de Dados

A camada de dados inclui atividades como ingestão de dados, engenharia de dados e transformação de dados usando Linguagem de Consulta Estruturada (SQL) ou tecnologias No SQL com bancos de dados/armazéns tradicionais ou tecnologias de Big Data. Os bancos de dados baseados em SQL oferecem segurança em nível de linha, coluna e célula. As tecnologias de big data anteriores ofereciam apenas segurança de nível de sistema de arquivo ou de sistema operacional (OS), mas agora oferecem segurança de nível inferior, por exemplo, o Apache Sentry[9] com autorização baseada em função.

As subcamadas de segurança nesta camada incluem segurança de rede, autenticação e autorização, mascaramento e/ou criptografia padrão da indústria de armazenamento de dados e gerenciamento de dados. O gerenciamento de dados comanda uma discussão separada, mas inclui arquitetura de dados corporativos, linhagem de dados, auditoria e governança. Uma má arquitetura de dados e/ou gerenciamento deficiente da linhagem de dados poderia comprometer a consistência e a disponibilidade dos dados.

A confidencialidade precisa ser mantida aderindo a vários padrões da indústria, como a Lei de Portabilidade de Seguros de Saúde e Responsabilidade dos EUA

(HIPAA) e o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) que regem o armazenamento, acesso e transmissão de dados. Um artigo anterior do *ISACA® Journal*, "De Volta para o Futuro em Segurança de Dispositivo: Alavancagem dos FIPPs para Gerenciar Proativamente o Risco de Privacidade e Segurança de IoT"[10] explica o design para considerações de privacidade no processamento de dados gerados a partir de componentes IoT.

Segurança da Camada de Business Intelligence

O mascaramento de dados, a autorização baseada em função e a autenticação única (SSO) fornecem segurança nessa camada, além da segurança de rede e firewalls. A gestão de modelo BI (preditivo, prescritivo) é um tópico de governança da informação. São necessários testes e validação suficientes para esses modelos. O uso de inteligência defeituosa pode levar a decisões de negócios mal embasadas, o que pode arruinar a reputação e a credibilidade de uma organização.

As tecnologias de prevenção de perda de dados (DLP) e de backup precisam ser consideradas para segurança adicional.

Segurança da Camada de Operações e Estratégia (OpS)

Um loop de feedback pode existir de aplicações/sistemas de operação para os dispositivos. A segurança de rede e firewalls tradicionais, o acesso e autorizações de aplicativos baseados em função e a SSO oferecem segurança nessa camada.

As ferramentas DevOps minimizam o risco de uma compilação incorreta e/ou má configuração, o que poderia afetar a disponibilidade do sistema.
Uma estratégia pode decidir um curso de ação baseado em resultados de BI. Uma estratégia pode ser apenas monitoramento de dados recebidos de dispositivos IoT, ou pode incluir processamento de dados recebidos de dispositivos IoT e alterar o comportamento de dispositivos IoT com base em limites aceitáveis de leituras de dados dos dispositivos. Tanto a estratégia (exigência e design) como o loop de feedback (implementação) precisam ser validados/testados.

> **“Um mau funcionamento do dispositivo pode afetar a disponibilidade e a integridade (qualidades básicas da segurança da informação) da segurança de IoT.”**

Modelagem de Ameaças e Gestão de Riscos

Figura 2 mostra um loop de feedback opcional desde a camada OpS até a camada de borda. Nos casos em que o loop de feedback esteja faltando e os dados dos dispositivos sejam considerados não sensíveis, o acesso aos dados e a segurança de criptografia podem ser reduzidos em conformidade com o gerenciamento de risco apropriado.
As estratégias de mitigação e resposta ao risco podem basear-se nas seguintes questões:

- Um dispositivo comprometido pode comprometer outros dispositivos ou o hub?
- Com que rapidez um dispositivo comprometido pode ser detectado e isolado?
- Qual é o impacto de um dispositivo comprometido?

Estas questões não são abrangentes e devem ser usadas como orientação inicial para a gestão de riscos.

Conclusão

A segurança de IoT muitas vezes não tem prioridade quando sistemas de IoT estão sendo projetados e

> **"A segurança de IoT não significa apenas segurança de nível do dispositivo; ela deve ser aplicada em todos os componentes e camadas do sistema de IoT."**

implementados. A segurança de IoT não significa apenas segurança de nível do dispositivo; ela deve ser aplicada em todos os componentes e camadas do sistema de IoT. A segurança deve ser abordada em todos os estágios do ciclo de vida do sistema de IoT, incluindo a fase de projeto, instalação, configuração e operação.

Adicionalmente, senhas e chaves de certificação fortes, dispositivo ou nomes/identificadores de host difíceis de serem adivinhados, monitoramento e análise de log, gestão pró-ativa de usuário e dispositivo e adesão aos guias do setor e recomendações de segurança de organizações como o Instituto Nacional de Padrões e Tecnologia dos EUA e a Organização Internacional para Padronização complementarão a segurança do sistema de IoT.

Notas Finais

1 Inteligência Empresarial, "Here's How the Internet of Things Will Explode by 2020," *Business Insider*, 31 August 2016, *www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-2*

2 Bacon, M.; "St. Jude Medical Finally Patches Vulnerable Medical IoT Devices," *TechTarget*, 13 January 2017, *http://searchsecurity.techtarget.com/news/450410935/St-Jude-Medical-finally-patches-vulnerable-medical-IoT-devices*

3 Golson, J.; "Car Hackers Demonstrate Wireless Attack on Tesla Model S," *The Verge*, 19 September 2016, *www.theverge.com/2016/9/19/12985120/tesla-model-s-hack-vulnerability-keen-labs*

4 Zorz, Z.; "Researchers Hack Vizio Smart TVs to Access Home Network," *Help Net Security*, 12 November 2015, *https://www.helpnetsecurity.com/2015/11/12/researchers-hack-vizio-smart-tvs-to-access-home-network/*

5 ForeScout, IoT Security Survey Results, *https://www.forescout.com/iot-security-survey-results/*

6 *Ibid*.

7 Zachman, J.; "The Concise Definition of the Zachman Framework," Zachman International Enterprise Architecture, 2008, *https://www.zachman.com/about-the-zachman-framework*

8 Eclipse, MQTT and CoAP, IoT Protocols, *www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php*

9 Sentry, Apache Sentry, *http://sentry.apache.org/*

10 Rotman, D.; C. Kypreos; S. Pipes; "Back to the Future in Device Security: Leveraging FIPPs to Proactively Manage IoT Privacy and Security Risk," *ISACA® Journal*, vol. 6, 2015, *https://www.isaca.org/Journal/archives*