Protegendo a Internet das Coisas (IoT) com a AWS

Adoção segura da nuvem

Abril de 2019

Avisos

Este documento é fornecido apenas para fins informativos. O documento representa as atuais ofertas de produtos e as práticas da AWS vigentes na data de emissão deste documento, que estão sujeitas a alterações sem aviso prévio. Os clientes são responsáveis, independentemente, por fazer suas próprias avaliações das informações contidas neste documento e por fazer qualquer uso dos produtos ou serviços da AWS, cada um dos quais é fornecido "no estado em que se encontram", sem qualquer tipo de garantia, seja expressa ou implícita. Este documento não cria quaisquer garantias, representações, compromissos contratuais, condições ou promessas da AWS, de suas afiliadas, fornecedores ou licenciadores. As responsabilidades e obrigações da AWS para com seus clientes são controladas por contratos da AWS, e este documento não faz parte de, nem modifica, nenhum contrato entre a AWS e seus clientes.

Conteúdo

Propósito

Este whitepaper é uma visão detalhada dos serviços de Internet das Coisas (IoT) com habilitação de segurança que os clientes podem aproveitar na Nuvem da AWS. Este paper destina-se a gerentes de programas de nível sênior, tomadores de decisões e profissionais de segurança que estão considerando a adoção segura de soluções de IoT para empresas.

Contexto

A tecnologia de IoT permite que as organizações otimizem os processos, aprimorem as ofertas de produtos e transformem as experiências dos clientes de várias maneiras. Embora os líderes de negócios estejam entusiasmados sobre como seus negócios podem se beneficiar dessa tecnologia, as preocupações de segurança, risco e privacidade permanecem. Isso ocorre, em parte, devido a um conflito com ofertas de segurança sem sentido, incompatíveis e, às vezes, imaturas, que não conseguem proteger adequadamente as implantações, colocando em risco crescente os dados do cliente ou do proprietário da empresa.

As organizações estão ansiosas para fornecer serviços inteligentes que possam melhorar drasticamente a qualidade de vida das populações, operações e inteligência de negócios, qualidade dos cuidados dos prestadores de serviços, resiliência de cidades inteligentes, sustentabilidade ambiental e uma série de cenários que ainda não foram imaginados. Mais recentemente, a AWS tem visto um aumento na adoção da IoT pelo setor de saúde e dos municípios, com a expectativa de que outras indústrias façam o mesmo no curto prazo. Muitos municípios foram os primeiros a adotar a tecnologia e estão assumindo a liderança quando se trata de integrar tecnologias modernas, como a IoT. Por exemplo:

- **Cidade do Kansas, Missouri:** A cidade do Kansas criou uma plataforma unificada de cidade inteligente para gerenciar novos sistemas que operam ao longo de seu corredor de bonde. Sensores de vídeo, sensores de pavimento, iluminações de rua conectadas, uma rede Wi-Fi pública e gerenciamento de estacionamento e tráfego suportaram uma redução de 40% nos custos de energia, US$ 1,7 bilhão no novo desenvolvimento do centro da cidade e 3.247 novas unidades residenciais.
- **Cidade de Chicago, Illinois:** Chicago está instalando sensores e câmeras em cruzamentos para detectar a quantidade de pólen e a qualidade do ar para seus cidadãos.
- **Cidade de Catânia, Itália:** Catânia desenvolveu um aplicativo para informar às pessoas onde fica a vaga de estacionamento disponível mais próxima a caminho do seu destino.
- **Cidade do Recife, Brasil:** Recife usa dispositivos de rastreamento colocados em cada caminhão de coleta de resíduos e carrinho de limpeza. A cidade conseguiu reduzir os custos de limpeza em US$ 250.000 por mês, ao mesmo tempo em que melhorou a confiabilidade do serviço e a eficiência operacional.
- **Cidade de Newport, em País de Gales, Reino Unido:** Newport implantou soluções de IoT de cidades inteligentes para melhorar a qualidade do ar, o controle de inundações e o gerenciamento de resíduos em poucos meses.
- **Jakarta, Indonésia:** Uma cidade de 28 milhões de habitantes que muitas vezes lida com inundações, Jakarta está tirando proveito da IoT para detectar níveis de água em canais e terras baixas, e está usando as mídias sociais para medir o sentimento dos cidadãos. Jakarta também é capaz de fornecer alerta antecipado e evacuação a bairros específicos para que o governo e os socorristas saibam quais áreas são as mais

necessitadas e possam coordenar o processo de evacuação.

De acordo com o Machina Research, o mercado global de IoT atingirá US$ 4,3 trilhões até 2024.[1] De acordo com o relatório do Departamento de Negócios, Inovação e Competências do Reino Unido (BIS UK), o mercado global de soluções para cidades inteligentes e os serviços adicionais necessários para implantá-las é estimado em US$ 408 bilhões até 2020[2]. Além disso, a Forbes[3] calcula que "manutenção preditiva, produção auto-otimizada e gerenciamento automatizado de inventário são os três principais casos de uso que impulsionam o crescimento do mercado de IoT até 2020". A Forbes afirma que as empresas querem aproveitar fornecedores de TI estabelecidos, maduros e com infraestrutura confiável ao criar ou implantar soluções de IoT devido à magnitude do impacto no cliente.

Embora os clientes estejam ansiosos para aproveitar as oportunidades de negócios disponíveis por meio da IoT, historicamente, a adoção segura da IoT não tem sido clara. Os recursos e serviços que permitem soluções nem sempre foram seguros por padrão, deixando potenciais lacunas de segurança nas bases arquitetônicas. Além disso, atualizações e manutenção não eram automáticas em práticas essenciais, como comunicações criptografadas e atualizações over-the-air (OTA). Por último, poucos provedores suportavam a capacidade de que dispositivos e gateways fossem corrigidos remotamente após a implantação, deixando esses dispositivos suscetíveis a riscos de segurança emergentes.

Em contraste, a AWS leva a segurança muito a sério, oferecendo suporte a milhões de clientes ativos de uma ampla variedade de setores e regiões geográficas, com vários requisitos de discrição de dados e confidencialidade. A AWS investe recursos significativos para garantir que a segurança seja incorporada em cada camada de seus serviços, estendendo essa segurança para dispositivos com IoT. Ajudar a proteger a confidencialidade, a integridade e a disponibilidade dos sistemas e dados do cliente ao mesmo tempo em que fornece uma plataforma segura, escalável e protegida para soluções IoT é uma prioridade para a AWS.

Desafios de segurança

Os riscos e vulnerabilidades de segurança têm o potencial de comprometer a segurança e a privacidade dos dados dos clientes em um aplicativo de IoT. Com o número crescente de dispositivos e os dados gerados, o potencial de danos levanta dúvidas sobre como abordar os riscos de segurança gerados por dispositivos de IoT e comunicação de dispositivos de e para a nuvem.

As preocupações comuns de clientes em relação aos riscos se centram na segurança e na criptografia de dados enquanto estão em trânsito de e para a nuvem, ou em trânsito de serviços de borda de e para o dispositivo, com patches de dispositivos, autenticação de dispositivos e usuários e controle de acesso. Proteger dispositivos de IoT é essencial, não só para manter a integridade dos dados, mas também para proteger contra ataques que possam afetar a confiabilidade dos dispositivos. Como os dispositivos podem enviar grandes quantidades de dados confidenciais por meio da internet, e os usuários finais têm poderes para controlar diretamente um dispositivo, a segurança das "coisas" deve permear cada camada da solução.

As notícias sobre comprometimento de dados colocam a segurança da IoT sob escrutínio adicional por parte dos clientes, mostrando lições aprendidas e incentivando práticas recomendadas. A base de uma solução de IoT deve

[1] De acordo com https://machinaresearch.com/news/the-global-iot-market-opportunity-will-reach-usd43-trillion-by-2024.

[2] Veja https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/249423/bis-13-1217 - smart-city-market-oportunties-uk.pdf.

[3] Veja https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by - 2020 / #74c8f8c7609b.

começar e terminar com segurança, com o uso de serviços capazes de auditar continuamente as configurações de IoT[4] para garantir que elas não se desviem das práticas recomendadas de segurança. Uma vez detectado um desvio, os alertas devem ser levantados para que as ações corretivas apropriadas possam ser implementadas — de preferência, automaticamente.

Para acompanhar a chegada de dispositivos ao mercado, bem como as ameaças on-line, a melhor solução é implementar serviços que abordem cada parte do ecossistema da IoT e se sobreponham em sua capacidade de garantir e proteger, auditar e corrigir, e gerenciar implantações de frotas de dispositivos de IoT (com ou sem conexão à nuvem).

Como os governos lidam com a segurança da IoT?

Enquanto as organizações do setor privado estão implantando ativamente a IoT em casos de uso como cuidados de saúde, construção industrial e produtos de baixo consumo de energia, governos nacionais e locais estão começando a lidar com a adoção e a segurança da IoT (consulte o Apêndice 2). Além de avaliar o cenário de políticas futuras da IoT, a AWS continua adicionando serviços a várias estruturas de conformidade para ajudar os clientes a cumprir suas obrigações de conformidade (consulte o Apêndice 3).

Serviços e recursos de segurança da IoT da AWS

A AWS oferece um conjunto de serviços de IoT para ajudar os clientes a proteger seus dispositivos, conectividade e dados. Esses serviços permitem que os clientes aproveitem a segurança ponta a ponta, da proteção do dispositivo aos dados em trânsito e em repouso. Eles também fornecem recursos que permitem a aplicação e a execução das políticas de segurança necessárias que atendam a seus mais altos padrões.

A IoT da AWS oferece funcionalidade ampla e profunda; clientes podem criar soluções de IoT para praticamente qualquer caso de uso em uma ampla variedade de dispositivos. A IoTda AWS se integra aos serviços de inteligência artificial (IA) para que os clientes possam tornar os dispositivos mais inteligentes — mesmo sem conectividade com a internet. Desenvolvido na Nuvem da AWS e usado por milhões de clientes em 190 países, a IoT da AWS pode ser facilmente dimensionada conforme as frotas de dispositivos dos clientes crescem e os requisitos de seus negócios evoluem. A IoT da AWS também oferece recursos abrangentes de segurança para que os clientes possam criar políticas de segurança preventivas e responder imediatamente a potenciais problemas de segurança.

[4] Uma configuração é um conjunto de controles técnicos definidos pelos clientes para ajudar a manter as informações protegidas quando os dispositivos estão se comunicando uns com os outros e com a nuvem.

A IoT da AWS fornece serviços em nuvem e software de borda, permitindo que os clientes conectem dispositivos com segurança, coletem dados e tomem ações inteligentes localmente, mesmo sem conectividade com a internet. Os serviços em nuvem permitem que os clientes rapidamente integrem e conectem com segurança frotas grandes e diversas, mantenham-as íntegras e seguras, e detectem e respondam a eventos dos sensores e aplicativos de IoT. Para acelerar o desenvolvimento de aplicativos de IoT, os clientes podem conectar facilmente dispositivos e serviços da Web usando uma interface de arrastar e soltar. A IoT da AWS também pode ser usada para analisar dados e criar modelos sofisticados de Aprendizado de Máquina. Esses modelos podem ser implantados na nuvem ou em dispositivos do cliente para tornar os dispositivos mais inteligentes.

Embora os atuais serviços da IoT da AWS[5] sejam amplamente variados para permitir soluções de IoT inovadoras e abrangentes, este whitepaper se concentra nos cinco serviços a seguir, que são a base para a segurança da IoT. As descrições de serviço e os recursos de segurança são discutidos abaixo.

- O **FreeRTOS da Amazon** é um sistema operacional de código aberto para microcontroladores que facilita a programação, a implantação, a proteção, a conexão e o gerenciamento de dispositivos de borda pequenos e de baixo consumo de energia.
- O **IoT Greengrass da AWS** é um software que permite que os clientes executem recursos locais de computação, mensagens, cache de dados, sincronização e inferência de ML em dispositivos conectados.
- O **IoT Core da AWS** é um serviço de nuvem gerenciada que permite que dispositivos conectados interajam com facilidade e segurança com aplicativos em nuvem e outros dispositivos.
- O **IoT Device Management da AWS** é um serviço de gerenciamento de dispositivos baseado na nuvem que facilita a integração, organização, monitoramento e gerenciamento remoto de dispositivos de IoT em escala com segurança.
- O **IoT Device Defender da AWS** é um serviço de segurança de IoT que continuamente monitora e audita as configurações de IoT do cliente para garantir que elas não se desviem das práticas recomendadas de segurança.

FreeRTOS da Amazon — Software de dispositivo

Visão geral do serviço: O FreeRTOS (a: FreeRTOS) da Amazon é um sistema operacional de código aberto para microcontroladores[6] que facilita a programação, a implantação, a proteção, a conexão e o gerenciamento de dispositivos de borda pequenos e de baixo consumo de energia. O Amazon FreeRTOS é baseado no kernel FreeRTOS, um sistema operacional popular de código aberto para microcontroladores, que o estende com bibliotecas de software que facilitam a conexão segura dos dispositivos pequenos e de baixo consumo de energia dos clientes diretamente aos serviços da Nuvem AWS , como o IoT Core da AWS , ou para dispositivos de borda mais poderosos que executam o IoT Greengrass da AWS .

[5] Os serviços de IoT da AWS incluem Amazon FreeRTOS, IoT Greengrass, IoT Core, IoT Device Management, IoT Device Defender, IoT Things Graph, IoT Analytics, IoT SiteWise e IoT Events. Para obter mais informações, visite https://aws. amazon.com/iot.

[6] Um microcontrolador é um chip único contendo um processador simples que pode ser encontrado em muitos dispositivos, incluindo aparelhos, rastreadores de fitness, sensores de automação industrial e automóveis. Muitos desses pequenos dispositivos podem se beneficiar da conexão à nuvem ou localmente a outros dispositivos. Por exemplo, medidores de eletricidade inteligentes precisam se conectar à nuvem para enviar relatórios de gasto, e sistemas de segurança de edifícios precisam se comunicar localmente para que uma porta seja destrancada quando alguém usar um crachá de acesso.

Recursos de segurança: O FreeRTOS da Amazon vem com bibliotecas para ajudar a proteger dados e conexões de dispositivos, incluindo suporte para criptografia de dados e gerenciamento de chaves. O Amazon FreeRTOS inclui suporte para Transport Layer Security (TLS v1.2) para ajudar os dispositivos a se conectarem com segurança à nuvem. O Amazon FreeRTOS também possui um recurso de assinatura de código para garantir que o código do dispositivo do cliente não seja comprometido durante a implantação, bem como recursos para atualizações OTA para atualizar dispositivos remotamente com aprimoramentos de recursos ou patches de segurança.

IoT Greengrass da AWS — Software para computação de borda

Visão geral do serviço: O IoT Greengrass da AWS é um software que permite que os clientes executem recursos locais de computação, mensagens, cache de dados, sincronização e inferência de ML para dispositivos conectados[7], permitindo que eles operem mesmo com conectividade intermitente com a nuvem. Depois que o dispositivo se reconecta, o IoT Greengrass da AWS sincroniza os dados no dispositivo com o IoT Core da AWS, fornecendo funcionalidade constante, independentemente da conectividade. O IoT Greengrass da AWS estende continuamente a AWS aos dispositivos para que eles possam agir localmente com base nos dados gerados, enquanto ainda usam a nuvem para gerenciamento, análise e armazenamento durável.

Recursos de segurança: O IoT Greengrass da AWS autentica e criptografa dados de dispositivos para comunicações locais e na nuvem, e os dados nunca são trocados entre dispositivos e a nuvem sem identidade comprovada. O serviço usa gerenciamento de segurança e acesso semelhante ao que os clientes estão familiarizados no IoT Core da AWS, com autenticação e autorização mútua de dispositivos e conectividade segura com a nuvem.

Mais especificamente, o IoT Greengrass da AWS usa certificados X.509[8], assinaturas gerenciadas, políticas de IoT da AWS e políticas e funções do Identity and Access Management (IAM) da AWS para garantir que os aplicativos do IoT Greengrass da AWS estejam protegidos. Os dispositivos de IoT da AWS exigem uma coisa da IoT da AWS, um certificado de dispositivo, e uma política de IoT da AWS para se conectar ao serviço IoT Greengrass da AWS. Isso permite que os principais dispositivos do IoT Greengrass da AWS se conectem com segurança ao serviço de nuvem da IoT da AWS. Ele também permite que o serviço de nuvem do IoT Greengrass da AWS implante informações de configuração, funções do Lambda da AWS e assinaturas gerenciadas em dispositivos principais do IoT Greengrass da AWS. Além disso, o IoT Greengrass da AWS fornece raiz de hardware de armazenamento de chave privada de confiança para dispositivos de borda.

Outros recursos de segurança importantes do IoT Greengrass da AWS são monitoramento e logging (registro). Por exemplo, o software principal no serviço pode gravar logs no Amazon CloudWatch[9] (que também funciona para o IoT Core da AWS) e no sistema de arquivos local dos dispositivos principais dos clientes. O logging é configurado a

[7] Para começar a usar o IoT Greengrass da AWS, os clientes precisarão de um dispositivo capaz de executar o núcleo do IoT Greengrass da AWS. Há uma lista completa de dispositivos qualificados e dependências técnicas aqui. Clique aqui para obter um guia prático de introdução. Os clientes podem encontrar a referência detalhada do desenvolvedor aqui.

[8] Os certificados X.509 são certificados digitais que usam o padrão de infraestrutura de chave pública X.509 para associar uma chave pública a uma identidade contida em um certificado. Os certificados X.509 são emitidos por uma entidade confiável chamada autoridade de certificação (AC). A AC mantém um ou mais certificados especiais chamados certificados de AC que usa para emitir certificados X.509. Somente a autoridade de certificação tem acesso a certificados de AC. Consulte https://docs.aws.amazon.com/iot/latest/developerguide/x509-certs.html para obter mais informações.

[9] Veja https://aws.amazon.com/cloudwatch.

nível de grupo e todos as entradas de log do IoT Greengrass da AWS incluem um carimbo de data/hora, nível de log e informações sobre o evento. O IoT Greengrass da AWS é integrado ao CloudTrail[10] da AWS — um serviço que fornece um registro das ações realizadas por um usuário, função ou um serviço da AWS no IoT Greengrass da AWS — e, se ativado pelo cliente, captura todas as chamadas da interface de programação de aplicativos (API) para o IoT Greengrass da AWS como eventos. Isso inclui chamadas do console do IoT Greengrass da AWS e chamadas de código para as operações de API do IoT Greengrass da AWS. Por exemplo, os clientes podem criar uma trilha e as chamadas podem permitir a entrega contínua de eventos do CloudTrail da AWS para o bucket de um Simple Storage Service (Amazon S3) da Amazon, incluindo eventos para o IoT Greengrass da AWS. Se os clientes não quiserem criar uma trilha, poderão visualizar os eventos mais recentes no console do CloudTrail da AWS por meio do histórico de eventos (se habilitado). Essas informações podem ser usadas para fazer várias coisas, como determinar quando uma solicitação foi feita para o IoT Greengrass da AWS e o endereço IP a partir do qual a solicitação foi feita.

Opções de práticas recomendadas estão disponíveis para proteger os dados dos clientes no dispositivo e devem ser utilizadas sempre que possível. Para o IoT Greengrass da AWS, todos os dispositivos de IoT devem habilitar a criptografia total do disco e seguir as práticas recomendadas de gerenciamento de chaves. Os clientes podem utilizar criptografia total de disco, usando chaves AES de 256 bits com base em algoritmos validados NIST FIPS 140-2[11] e seguir as práticas recomendadas de gerenciamento de chaves. Para dispositivos de baixa potência, como aqueles que usam o FreeRTOS da Amazon, os clientes podem seguir as recomendações de criptografia leve[12] do NIST 8114.

As seções acima cobriram microcontroladores e casos de uso de borda. Abaixo, o artigo se concentrará em serviços de IoT que operam na nuvem.

[10] Veja https://aws.amazon.com/cloudtrail.

[11] Algoritmos criptográficos aprovados NIST FIPS 140-2: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/ documents/fips1402annexa .pdf.

[12] NIST 8114 — Criptografia leve: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

IoT Core da AWS — Gateway de IoT baseado em nuvem

Visão geral do serviço: O IoT Core da AWS é um serviço na nuvem gerenciado que permite, de forma fácil e segura, a interação de dispositivos conectados com aplicativos na nuvem e com outros dispositivos. O IoT Core da AWS fornece comunicação segura e processamento de dados em diferentes tipos de dispositivos conectados e locais para que os clientes possam criar facilmente aplicativos de IoT. Exemplos de casos de uso do cliente incluem soluções industriais e soluções domésticas conectadas, com a capacidade de suportar bilhões de dispositivos e trilhões de mensagens que podem ser processadas e roteadas para endpoints da AWS e outros dispositivos de forma confiável e segura.

Recursos de segurança: O IoT Core da AWS oferece várias soluções aos clientes que ajudam a habilitar e manter a segurança. Os mecanismos de segurança na Nuvem da AWS protegem os dados à medida que eles se movem entre a IoT da AWS e outros dispositivos ou serviços da AWS . Os dispositivos podem se conectar usando uma variedade de opções de identidade (certificados X.509, usuários e grupos de IAM, identidades do Amazon Cognito ou tokens de autenticação personalizados) em uma conexão segura.
Enquanto os clientes realizam as validações do lado do cliente (ou seja, validação de cadeia de confiança, verificação de nome de host, armazenamento seguro e distribuição de suas chaves privadas), o IoT Core da AWS fornece canais de transporte seguros usando o TLS. O mecanismo de regras da IoT da AWS também encaminha dados do dispositivo para outros dispositivos e serviços da AWS de acordo com as regras definidas pelo cliente. Os sistemas de gerenciamento de acesso da AWS são usados para transferir dados com segurança para seu destino final. Outro recurso de autorização da IoT da AWS que merece destaque são as variáveis de política da IoT da AWS , que ajudam a evitar o provisionamento de credenciais com privilégios excessivos para um dispositivo. Esses recursos, usados em conjunto com as práticas recomendadas gerais de segurança cibernética, ajudam a proteger os dados dos clientes.

IoT Device Management da AWS — Serviço de gerenciamento de dispositivos de IoT baseado em nuvem

Visão geral do serviço: O IoT Device Management da AWS ajuda os clientes a integrar, organizar, monitorar e gerenciar remotamente dispositivos de IoT em escala. O IoT Device Management da AWS integra-se ao IoT Core da AWS para conectar facilmente dispositivos à nuvem e a outros dispositivos para que os clientes possam gerenciar remotamente suas frotas de dispositivos. O IoT Device Management da AWS ajuda os clientes a integrar novos dispositivos usando a IoT da AWS no Management Console da AWS ou em uma API para carregar modelos que eles preenchem com informações como fabricante e número de série do dispositivo, certificados de identidade X.509 ou políticas de segurança. Depois disso, os clientes podem configurar toda a frota de dispositivos com essas informações com alguns cliques na IoT da AWS no Management Console da AWS.

Recursos de segurança: Com o IoT Device Management da AWS, os clientes podem agrupar sua frota de dispositivos em uma estrutura hierárquica com base em funções, requisitos de segurança ou categorias semelhantes. Eles podem agrupar um único dispositivo em uma sala, vários dispositivos no mesmo andar ou todos os dispositivos que operam dentro de um edifício. Esses grupos podem ser usados para gerenciar políticas de acesso, visualizar métricas operacionais ou executar ações em todo o grupo. Além disso, um recurso conhecido como “Dynamic Things” pode adicionar automaticamente dispositivos que atendam aos critérios definidos pelo cliente e remover dispositivos que

não correspondam mais aos requisitos. Isso simplifica o processo com segurança, mantendo a integridade operacional. O Dynamic Things também facilita a localização de registros de dispositivos com base em qualquer combinação de atributos de dispositivo e permite que os clientes executem atualizações em massa.

Com o IoT Device Management da AWS, os clientes também podem enviar software e firmware para dispositivos em campo para corrigir vulnerabilidades de segurança e melhorar a funcionalidade do dispositivo, executar atualizações em massa, controlar a velocidade da implantação, definir limites de falha e definir tarefas contínuas para atualizar o software do dispositivo automaticamente para que eles estejam sempre executando a versão mais recente do software. Os clientes podem enviar ações remotamente, como reinicializações de dispositivo ou restaurações de fábrica, para corrigir problemas de software no dispositivo ou restaurar o dispositivo para suas configurações originais. Os clientes também podem assinar digitalmente arquivos enviados para seus dispositivos, ajudando a garantir que os dispositivos não sejam comprometidos.

A capacidade de enviar atualizações de software não se limita aos serviços de nuvem. Na verdade, as tarefas de atualização OTA no FreeRTOS da Amazon permitem que os clientes usem o IoT Device Management da AWS para agendar atualizações de software. Da mesma forma, os clientes também podem criar uma tarefa de atualização principal do IoT Greengrass da AWS para um ou mais dispositivos principais do IoT Greengrass da AWS usando o IoT Device Management da AWS para implantar atualizações de segurança, correções de bugs e novos recursos do IoT Greengrass da AWS para dispositivos conectados.

IoT Device Defender da AWS — Serviço de segurança de dispositivo de IoT baseado em nuvem

Visão geral do serviço: O IoT Device Defender da AWS é um serviço totalmente gerenciado que ajuda os clientes a auditar os recursos de segurança estabelecidos para sua frota de dispositivos de IoT. O serviço audita continuamente as configurações de IoT para garantir que as configurações não se desviem das práticas recomendadas de segurança para manter e aplicar configurações de IoT — como garantir a identidade do dispositivo, autenticar e autorizar dispositivos e criptografar dados do dispositivo. O serviço pode enviar um alerta se houver lacunas na configuração de IoT de um cliente que possa criar um risco de segurança, como certificados de identidade sendo compartilhados em vários dispositivos ou um dispositivo com um certificado de identidade revogado tentando se conectar ao IoT Core da AWS.

Recursos de segurança: Além dos recursos de monitoramento e auditoria do serviço, os clientes podem definir alertas que tomam medidas para corrigir quaisquer desvios encontrados nos dispositivos. Por exemplo, picos no tráfego de saída podem indicar que um dispositivo está participando de um ataque de negação de serviço distribuído (DDoS). O IoT Greengrass da AWS e o FreeRTOS da Amazon também se integram automaticamente ao IoT Device Defender da AWS para fornecer métricas de segurança dos dispositivos para avaliação.

O IoT Device Defender da AWS pode enviar alertas para a IoT da AWS, CloudWatch da Amazon e Simple Notification Service (Amazon SNS) da Amazon, com alertas sendo publicadas nas métricas do CloudWatch da Amazon. Se um cliente decidir lidar com um alerta, o IoT Device Management da AWS pode ser usado para executar ações atenuantes, como enviar correções de segurança.

O IoT Device Defender da AWS audita configurações de IoT associadas a dispositivos do cliente em um conjunto de

práticas recomendadas de segurança de IoT definidas para que os clientes possam ver onde existem lacunas de segurança e executar auditorias de forma contínua ou ad-hoc. Há também práticas de segurança no IoT Device Defender da AWS que podem ser selecionadas e executadas como parte da auditoria. Esse serviço também se integra a outros serviços da AWS, como o CloudWatch da Amazon e o SNS da Amazon, para enviar alertas de segurança para a IoT da AWS quando uma auditoria falha ou quando anomalias de comportamento são detectadas para que os clientes possam investigar e determinar a causa raiz. Por exemplo, o IoT Device Defender da AWS pode alertar os clientes quando as identidades de dispositivo estão acessando APIs confidenciais. O IoT Device Defender da AWS também pode recomendar ações que minimizem o impacto de problemas de segurança, como revogar permissões, reiniciar um dispositivo, redefinir padrões de fábrica ou enviar correções de segurança para qualquer um dos dispositivos conectados dos clientes.

Os clientes também podem estar preocupados com indivíduos mal-intencionados, erros humanos ou sistêmicos e usuários autorizados com intenções maliciosas que possam introduzir configurações com impactos negativos na segurança. O IoT Core da AWS fornece os blocos de construção de segurança para que os clientes conectem dispositivos com segurança à nuvem e a outros dispositivos. Os blocos de construção permitem a aplicação de controles de segurança, como autenticação, autorização, registro de auditoria e criptografia de ponta a ponta. Em seguida, o IoT Device Defender da AWS entra e ajuda a auditar continuamente as configurações de segurança para conformidade com as práticas recomendadas de segurança e as políticas de segurança organizacional dos clientes.

Aproveitando a segurança comprovada para aprimorar a IoT — um diferencial do setor

Novos serviços e tecnologias de segurança estão sendo criados na AWS para ajudar as empresas a proteger sua IoT e dispositivos de borda. Em particular, a AWS lançou recentemente verificações no IoT Device Defender da AWS com tecnologia de IA conhecida como raciocínio automatizado, que aproveita provas matemáticas para verificar se o software foi escrito corretamente e determinar se há acesso não intencional aos dispositivos. O IoT Device Defender da AWS é um exemplo de como os clientes podem usar diretamente o raciocínio automatizado para proteger seus próprios dispositivos. Internamente, a AWS usou raciocínio automatizado para verificar a integridade da memória do código em execução no FreeRTOS da Amazon e para proteger contra malware. O investimento em raciocínio automatizado para fornecer garantia escalável de software seguro, referido como "segurança comprovável", permite que os clientes operem cargas de trabalho confidenciais na AWS.

O Zelkova da AWS[13] usa raciocínio automatizado para comprovar que os controles de acesso a dados do cliente estão operando conforme deveriam. As verificações de controle de acesso no IoT Device Defender da AWS são alimentadas pelo Zelkova, permitindo que os clientes se assegurem de que seus dados estão protegidos adequadamente. Uma política de IoT da AWS é excessivamente permissiva se conceder acesso a recursos fora da configuração de segurança pretendida do cliente. Os controles alimentados pelo Zelkova incorporados no IoT Device Defender da AWS verificam se as políticas não permitem ações restritas pela configuração de segurança do cliente e que os recursos pretendidos têm permissões para executar determinadas ações.

[13] Para saber mais sobre o Zelkova, visite https://aws.amazon.com/blogs/security/protect-sensitive-data-in-the-cloud-with-automated - reasoning-zelkova.

Outras ferramentas baseadas em raciocínio automatizado têm ajudado a proteger as bases da infraestrutura de IoT da AWS. Uma ferramenta de código aberto chamada CBMC foi usada para comprovar a exatidão do FreeRTOS da Amazon, proporcionando maior confiança ao cliente para executar cargas de trabalho em dispositivos de IoT da Amazon. Isso garante que nenhum invasor possa explorar ou obter acesso não autorizado ao FreeRTOS da Amazon. Mecanismos de controle de raciocínio automatizado no FreeRTOS da Amazon foram continuamente integrados, assim como verificações de atualizações feitas no sistema operacional. Isso garante que cada vez que uma alteração de código for feita, medidas sejam implementadas, permitindo que os desenvolvedores da AWS possam verificar automaticamente se o software do FreeRTOS da Amazon é seguro para memória.

O raciocínio automatizado continua sendo implementado em uma variedade de serviços e recursos da AWS, fornecendo níveis elevados de garantia de segurança para componentes críticos da Nuvem AWS. A AWS continua implantando raciocínio automatizado para desenvolver ferramentas para clientes, bem como tecnologia de verificação de infraestrutura interna para a pilha da IoT da AWS.

Quais são as principais práticas recomendadas de segurança da IoT?

Apesar do número de práticas recomendadas disponíveis, não existe uma abordagem única para atenuar riscos em soluções de IoT. Dependendo do dispositivo, sistema, serviço e ambiente em que os dispositivos são implantados, existem diferentes ameaças, vulnerabilidades e tolerâncias de risco para os clientes considerarem. Aqui estão as práticas recomendadas ao incorporar segurança ponta a ponta em dados, dispositivos e serviços em nuvem:

1. **Incorporar segurança na fase de design**
   A base de uma solução de IoT começa e termina com segurança. Como os dispositivos podem enviar grandes quantidades de dados confidenciais, e os usuários finais de aplicativos de IoT também podem ter a capacidade de controlar diretamente um dispositivo, a segurança das "coisas" deve ser um requisito de design universal. A segurança não é uma fórmula estática; os aplicativos de IoT devem ser capazes de modelar, monitorar e iterar continuamente as práticas recomendadas de segurança. Um desafio para a segurança de IoT é o ciclo de vida de um dispositivo físico e o hardware restrito para sensores, microcontroladores, atuadores e bibliotecas incorporadas. Esses fatores restritos podem limitar os recursos de segurança que cada dispositivo pode executar. Com essas dinâmicas adicionais, as soluções de IoT devem adaptar continuamente sua arquitetura, firmware e software para se manter à frente do cenário de segurança em constante mudança. Embora os fatores restritos dos dispositivos possam apresentar maiores riscos, barreiras e potenciais compensações entre segurança e custo, criar uma solução segura de IoT deve ser o principal objetivo de qualquer organização.

2. **Construir com base em estruturas reconhecidas de segurança de TI e cibersegurança**
   A AWS oferece suporte a uma abordagem aberta e baseada em padrões para promover a adoção segura de IoT. Ao considerar os bilhões de dispositivos e pontos de conexão necessários para apoiar um ecossistema de IoT robusto para uso do consumidor, industrial e do setor público, a interoperabilidade é vital. Assim, os serviços de IoT da AWS aderem aos protocolos padrão do setor e às práticas recomendadas. Além disso, o IoT

Core da AWS oferece suporte a outros padrões do setor e protocolos personalizados, permitindo que dispositivos se comuniquem entre si mesmo que estejam usando protocolos diferentes. A AWS é um forte defensor da interoperabilidade para que os desenvolvedores possam criar sobre as plataformas existentes de modo a dar suporte às necessidades em evolução dos clientes. A AWS também oferece suporte a um ecossistema de parceiros próspero para expandir o menu de opções e ampliar os limites do que é possível para os clientes. A aplicação de práticas recomendadas reconhecidas no mundo todo traz uma série de benefícios a todas as partes interessadas da IoT, entre eles:

- Repetibilidade e reutilização, em vez de reiniciar e refazer
- Coerência e consenso para promover a compatibilidade da tecnologia e da interoperabilidade entre fronteiras geográficas
- Maximização da eficiência para acelerar a modernização e a transformação da TI

3. **Foco no impacto para priorizar medidas de segurança**

Ataques ou anormalidades não são idênticos e podem não ter o mesmo impacto em pessoas, operações comerciais e dados. Compreender os ecossistemas de IoT do cliente e onde os dispositivos operarão nesse ecossistema diz onde estão os maiores riscos — dentro do dispositivo, como parte da rede, ou componente físico ou segurança. Focar na avaliação de impacto de risco e consequências é fundamental para determinar onde os esforços de segurança devem ser direcionados, e quem será o responsável por esses esforços no ecossistema de IoT.

Conclusão

Junto com um crescimento exponencial em dispositivos conectados, cada "coisa" na IoT comunica pacotes de dados que exigem conectividade, armazenamento e segurança confiáveis. Com a IoT, uma organização é desafiada a gerenciar, a monitorar e a proteger imensos volumes de dados e conexões de dispositivos dispersos. Mas esse desafio não precisa ser um obstáculo em um ambiente baseado em nuvem. Além de dimensionar e expandir uma solução em um único local, a computação em nuvem permite que as soluções de IoT sejam dimensionadas globalmente e em diferentes locais físicos, reduzindo a latência da comunicação e permitindo uma melhor capacidade de resposta dos dispositivos no campo. A AWS oferece um conjunto de serviços de IoT com segurança ponta a ponta, incluindo serviços para operar e proteger endpoints, gateways, plataformas e aplicativos, bem como o tráfego que atravessa essas camadas. Essa integração simplifica o uso e o gerenciamento seguros de dispositivos e dados que interagem continuamente uns com os outros, permitindo que as organizações se beneficiem da inovação e eficiência que a IoT pode oferecer, mantendo a segurança como prioridade.

Apêndice 1 — Integração de serviços da IoT da AWS

A IoT da AWS integra-se diretamente aos seguintes serviços da AWS:

- O **Simple Storage Service (Amazon S3)** da **Amazon** fornece armazenamento escalável na Nuvem AWS. Para obter mais informações, consulte Amazon S3.
- O **DynamoDB da Amazon** fornece bancos de dados NoSQL gerenciados. Para obter mais informações, consulte Amazon DynamoDB.
- O **Kinesis** da **Amazon** permite o processamento em tempo real de dados de streaming em larga escala. Para obter mais informações, consulte Amazon Kinesis.
- O **Lambda** da **AWS** executa o código dos clientes em servidores virtuais do Elastic Compute Cloud (Amazon EC2) da Amazon em resposta a eventos. Para obter mais informações, consulte o Lambda da AWS.
- O **Simple Notification Service (Amazon SNS)** da **Amazon** envia ou recebe notificações. Para obter mais informações, consulte Amazon SNS.
- O **Simple Queue Service (Amazon SQS)** da **Amazon** armazena dados em uma fila a ser recuperada pelos aplicativos. Para obter mais informações, consulte Amazon SQS.

Apêndice 2 — Governos lidando com a IoT

Estados Unidos

Instituto Nacional de Normas e Tecnologia (NIST) — Departamento de Comércio

O Departamento de Comércio dos Estados Unidos está liderando vários esforços para lidar com a segurança da IoT. O Instituto Nacional de Normas e Tecnologia (NIST) publicou um whitepaper[14]que traz à luz tópicos que tanto clientes quanto agências governamentais consideram ao avaliar a segurança de dados e dispositivos. No whitepaper, os leitores são encorajados a avaliar essas preocupações e recebem recomendações sobre como mitigar os problemas. O NIST também lançou o seu Relatório Interno (NITIR) 8228[15], que identifica riscos que podem afetar negativamente a adoção da IoT. O documento também oferece recomendações para mitigar ou reduzir os efeitos dessas preocupações. O NIST também está convocando parcerias públicas e privadas, solicitando opiniões e organizando workshops relacionados a cidades inteligentes e padronização internacional da IoT, entre uma série de outras iniciativas[16]. Embora em sua fase inicial, os primeiros indicadores apontam para potenciais riscos de segurança cibernética e privacidade como sérios desafios para os ganhos que governos e consumidores podem obter por meio da IoT.

Departamento de Defesa

Outro exemplo dentro do governo é encontrado na comunidade de defesa. Em 2016, o diretor de TI do Departamento de Defesa (DoD) dos EUA emitiu recomendações de políticas para lidar com as vulnerabilidades e riscos da IoT[17]. De acordo com a recomendação da política, o DoD já usa milhões de dispositivos e sensores de IoT em instalações, veículos e dispositivos médicos do DoD e está considerando incorporá-los em armamentos e sistemas de inteligência. A complexidade de proteger a IoT decorre do poder de processamento limitado dos dispositivos para executar firewalls e antimalware, bem como do grande número de dispositivos, o que aumenta a exposição à vulnerabilidade a um nível diferente dos dispositivos móveis tradicionais.

A abordagem e a política que o DoD recomenda para lidar com os riscos de segurança da IoT incluem: 1) uma análise de risco de segurança e privacidade que suporte cada implementação de IoT e fluxos de dados associados, 2) criptografia em cada ponto, onde os custos são proporcionais ao risco e benefício, e 3) monitoramento de redes de IoT para identificar tráfego anormal e ameaça emergente.

Comissão Federal do Comércio (FTC)

[14] Jeffrey Voas (NIST), Richard Kuhn (NIST), Phillip Laplante (Penn State University) e Sophia Applebaum (MITRE), "Internet of Things (IoT) TrustConcerns" (16 de outubro de 2018, https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft.)

[15] NISTIR 8228, "Considerations for Managing IoT Cybersecurity and Privacy Risks Out for Public Comment" (26 de setembro de 2018, https://www.nist.gov/news-events/news/2018/09/draft-nistir-8228-considerations-managing-iot-cybersecurity-and-privacy.)

[16] Veja https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot.

[17] Veja https://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20 Internet% 200f% 20Things% 20-% 20White% 20Paper.pdf? ver = 2017-01-26-152811-440.

A FTC tem sido um participante importante nas conversas de segurança da IoT, tomando medidas contra fabricantes de dispositivos que tenham deturpado ou demonstrado negligência nos seus compromissos com a segurança. A FTC estipulou o próprio padrão para uma "segurança de dados razoável". A FTC identificou as seguintes deficiências de segurança repetidas nos fabricantes de dispositivos:

- Segurança não incorporada em dispositivos
- Os desenvolvedores não estão treinando seus empregados em boas práticas de segurança
- Não garantir a segurança e a conformidade no recebimento de informações (por meio de contratos)
- Falta de defesa em estratégias de profundidade
- Falta de controles de acesso razoáveis (os clientes podem ignorar ou tentar adivinhar senhas padrão)
- Falta de um programa de segurança de dados

Estado da Califórnia

A Califórnia está entre os primeiros estados nos Estados Unidos a aprovar legislação sobre a IoT. Os projetos de lei atuais abordam problemas como segurança do design do dispositivo e proteção de dados, mas não têm requisitos específicos para os fabricantes de produtos de IoT. Em vez disso, os legisladores têm se concentrado na segurança na fase de design, dizendo que a proteção dos dados deve ser "adequada à natureza e função do dispositivo" e "adequada às informações que ele pode coletar, conter ou transmitir".

Reino Unido

O Departamento para Digitais, Cultura, Mídia e Esporte (DCMS) do Reino Unido publicou a versão final do seu Código de Prática para Segurança de IoT do Consumidor em outubro de 2018[18]. Este Código de Prática foi elaborado em conjunto com o Centro Nacional de Segurança Cibernética e teve a contribuição de associações de consumidores, indústria e comunidade acadêmica. O documento fornece 13 diretrizes sobre como alcançar uma abordagem "segura por design" para todas as organizações envolvidas no desenvolvimento, fabricação e varejo de produtos de IoT de consumo.

O Código de Prática enfatiza três práticas principais para permitir que os usuários obtenham os maiores e mais imediatos benefícios de segurança, e insta as partes interessadas da IoT a priorizá-las: 1) Sem senhas padrão: Muitos usuários não alteram a senha padrão, o que tem sido a fonte de muitos problemas de segurança da IoT. 2) Implementar uma política de divulgação de vulnerabilidades: Os desenvolvedores de dispositivos, serviços e aplicativos de IoT devem ter uma política de divulgação de vulnerabilidades e um ponto de contato público para permitir o relato (e correção) de vulnerabilidades em tempo hábil. 3) Manter o software atualizado: As atualizações de software precisam ser oportunas e fáceis de implementar, e não devem interferir no funcionamento do dispositivo.

[18] Veja https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security.

Com base nas preocupações e abordagens delineadas pelos EUA e pelo Reino Unido, a segurança da IoT continuará a ser a prioridade para os governos. Esforços de organismos nacionais e internacionais de normalização também estão em curso para desenvolver padrões, diretrizes e práticas recomendadas para proteger a IoT[19], incluindo a Arquitetura de Referência de IoT da Organização Internacional de Normalização (ISO) e o grupo de estudo da União Internacional de Telecomunicações (ITU) sobre IoT e cidades inteligentes.[20]

No contexto da IoT, os clientes devem ter a flexibilidade de usar práticas existentes e testadas já em uso no que é considerado mais "segurança cibernética de rede tradicional". Por exemplo, ao tentar identificar vulnerabilidades, detectar irregularidades, responder a potenciais incidentes e recuperar danos ou interferências em dispositivos de IoT, os clientes podem usar os controles de segurança cibernética mapeados no Cybersecurity Framework (CSF) do NIST[21]. Este conjunto básico de disciplinas de segurança cibernética é reconhecido globalmente e tem sido apoiado por governos e indústrias como uma referência recomendada para uso por qualquer organização, independentemente de seu setor ou tamanho. A vantagem de utilizar o CSF do NIST não é apenas por sua reputação, mas também a flexibilidade que permite aplicar segurança cibernética tendo em mente seu efeito nas dimensões física, cibernética e de pessoas. Com o aspecto humano, a estrutura se aplica às organizações que dependem da tecnologia, quer o foco seja principalmente na tecnologia da informação, sistemas de controle industrial, sistemas ciber-físicos ou na IoT.

[19] Para obter um resumo de padrões atuais e iniciativas sobre segurança da IoT, consulte o catálogo da Administração Nacional de Telecomunicações e Informações (NTIA) do Departamento de Comércio dos EUA: https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_17.pdf.

[20] Veja https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx.

[21] Para obter detalhes adicionais sobre como alinhar com o CSF do NIST usando os serviços da AWS, consulte este whitepaper e manual do cliente: https://do.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf.

Apêndice 3 — Serviços e conformidade da IoT da AWS

Como um provedor global de serviços de nuvem em hiperescala, a AWS adota uma abordagem rigorosa e baseada em riscos para a segurança de seus serviços de IoT e a proteção dos dados dos clientes. A AWS faz cumprir processos de segurança interna em todos os seus serviços de nuvem para avaliar a eficácia dos controles gerenciais, técnicos e operacionais necessários para proteção contra ameaças de segurança atuais e emergentes que afetem a segurança e a resiliência. Esse processo de garantia de segurança obrigatório resulta não apenas na certificação de várias estruturas de conformidade, mas também dobra o compromisso da AWS de incorporar segurança em todas as fases do desenvolvimento e em todos os processos operacionais do ciclo de vida de seus serviços. A AWS oferece serviços de nuvem comercial em hiperescala que foram acreditados em relação aos padrões líderes reconhecidos internacionalmente, como a Organização Internacional de Normalização 27001 (ISO)[22], Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI)[23] e o Relatórios de Controle de Organização de Serviço (SOC)[24], entre outras certificações internacionais, nacionais e setoriais. A AWS também atende aos rigorosos requisitos de segurança em relação ao suporte a ambientes classificados de determinadas agências de inteligência. Em conjunto, os clientes de qualquer setor e de qualquer porte que usam os serviços da Nuvem da AWS obtêm benefícios de segurança por proxy, pois a AWS aplica o mais alto padrão em seus serviços.

A AWS está ciente de que os clientes podem ter requisitos específicos de conformidade que devem ser comprovados e cumpridos. Tendo isso em mente, a AWS adiciona continuamente serviços que se alinhem aos programas de conformidade com base na demanda do cliente. Os serviços de IoT no escopo são listados pelo programa de conformidade no site da AWS[25].

[22] A ISO 27001/27002 é um padrão de segurança global amplamente adotado que estabelece requisitos e práticas recomendadas para uma abordagem sistemática ao gerenciamento de informações da empresa e do cliente que se baseia em avaliações periódicas de risco adequadas a cenários de ameaça em constante mudança. A ISO 27018 é um código de prática que foca na proteção de dados pessoais na nuvem. Ele é baseado no padrão de segurança da informação ISO 27002 e fornece orientações de implementação sobre controles ISO 27002 aplicáveis às Informações Pessoais Identificáveis (PII) na nuvem pública. Ele também fornece um conjunto de controles adicionais e orientações associadas destinados a atender aos requisitos de proteção de PII na nuvem pública não atendidos pelo conjunto de controle ISO 27002 existente.

[23] O Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS) é um padrão de segurança de informações proprietário administrado pelo Conselho de Padrões de Segurança PCI (https://www.pcisecuritystandards.org), que foi fundado pela American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc. OPCI DSS aplica-se a todas as entidades que armazenam, processam ou transmitem dados de titulares de cartões (CHD) e/ou dados de autenticação sensível (SAD), incluindo comerciantes, processadores, adquirentes, emissores e provedores de serviços.

[24] Os Relatórios de Controles de Organização de Serviço (SOC 1, 2, 3) destinam-se a atender a uma ampla gama de requisitos de auditoria financeira para órgãos de auditoria dos EUA e internacionais. A auditoria deste relatório é realizada de acordo com as Normas Internacionais para Compromissos de Garantia No. 3402 (ISAE 3402) e o Instituto Americano de Contadores Públicos Certificados (AICPA): AT 801 (antigo SSAE 16).

[25] Ver https://aws.amazon.com/compliance/services-in-scope.