Sábado, 11 de Outubro de 2025

Proteger Dispositivos Conectados à IoT Torna a Internet Mais Segura

LUIZA DIAS

7 de fevereiro é o Dia da Internet Segura. Essa é uma campanha que destaca a importância de promover e concretizar uma internet mais segura.

Um fato interessante sobre a rede: existem quase 5 bilhões de usuários de internet ativos em todo o mundo. Isso configura um pouco mais de 60% da população total do mundo. Mas esse número fica pequeno em comparação com os 15 bilhões de dispositivos IoT (Internet das Coisas) esperados este ano, e uma projeção de 29 bilhões até 2030. A IoT está em toda parte, desde o monitoramento da rede de água e energia até os recursos de transporte e armazenamento dos quais dependemos; e de estabelecimentos de saúde monitorando os valores estatísticos dos pacientes aos nossos dispositivos de consumo, como smartphones, automóveis e eletrodomésticos.

Os Dispositivos IoT Estão Aumentando Significativamente As Superfícies de Ataque à Cibersegurança

À medida que o número de dispositivos IoT aumenta globalmente, suas vulnerabilidades também se intensificam. Os dispositivos da Internet das Coisas (IoT) são superfícies de ataque e vulneráveis a ameaças cibernéticas de rede, como roubo de dados, phishing, spoofing e ataques de negação de serviço. Compreender e identificar as diversas ameaças e vulnerabilidades dos dispositivos conectados à IoT pode ajudar as organizações a reduzir seus riscos.

Como os dispositivos IoT são predominantemente remotos, a atualização de software e firmware é um desafio contínuo. Muitos permanecem sem monitoramento e gerenciados de forma inadequada. Essa falta de visibilidade do status do dispositivo pode impedir que as organizações detectem ou mesmo respondam a possíveis ameaças.

As ameaças à segurança da IoT podem variar de simples violações de senha a ataques sofisticados que tiram proveito de vulnerabilidades de hardware e softwares desatualizados. O aumento do uso de IoT em redes em nuvem que armazenam e analisam dados é um possível risco para o crescimento no número de infrações, devido à falta de criptografia e controle de acesso. A proteção contra esses ataques pode ser realizada adicionando controles de identidade e criptografando os dados entre dispositivos IoT e serviços em nuvem.

Uma Ameaça Crescente Para as Tecnologias Industriais

Existem muitos dispositivos IoT localizados em instalações industriais que executam sistemas de Tecnologia Operacional (TO). Durante décadas, os domínios de TI e TO permaneceram completamente separados. Mas, com a ascensão da transformação digital e ampla utilização da Internet, os ambientes de TI e TO estão se fundindo.

Essa convergência aumenta a superfície de ataque de dispositivos e sistemas de TI e TO interconectados, criando vulnerabilidades que representam ameaças significativas. Essas fragilidades geram riscos para fabricantes industriais, petróleo e gás, transporte, sistemas de gerenciamento de água e resíduos, usinas de processamento de alimentos, serviços de eletricidade e outras instalações industriais.

A IoT Industrial (IIoT) tem sido fundamental na revolução conhecida como Indústria 4.0, a próxima fase da digitalização do setor manufatureiro. O ênfase da IIoT em interconectividade, automação, aprendizado de máquina e análise de dados em tempo real está impulsionando uma nova era de inovações de fabricação inteligente. Os benefícios, porém, devem ser equilibrados com maior vigilância para mitigar o aumento do cenário de ameaças criado pela implementação desses dispositivos conectados.

É Importante Revisar as Limitações de Segurança do Dispositivo e as Melhores Práticas

Antes de comprar ou implantar dispositivos IoT, é importante entender suas limitações de segurança, pois poucos fabricantes fornecem medidas de segurança robustas. Um novo requisito de padronização recentemente implementado para IoT pode promover maior adesão do fornecedor a disponibilização de protocolos de segurança maiores.

A falta de melhores práticas de segurança para esses dispositivos cria um risco de regressão para o ecossistema de IoT. No entanto, com uma solução de gerenciamento de identidade adequada, as organizações podem criar facilmente um ecossistema com reconhecimento de identidade que mapeia dispositivos IoT que a possuem. Isso permite que as empresas aproveitem a identidade para reforçar a segurança de acesso com rastreamento de dados auditáveis. A identidade de dispositivos IoT é um componente de segurança crítico para resguardar o ecossistema IoT. Prover e gerenciar identidades de dispositivos durante todo seu ciclo de vida ajuda a proteger contra ameaças de cibersegurança.

Dispositivos IoT Devem Ser Protegidos com Identidades de um Provedor Confiável

Para garantir um ecossistema seguro, cada dispositivo IoT deve ter uma identidade única. Isso garantirá autenticação adequada quando um dispositivo ficar online e comunicação criptografada confiável entre outros dispositivos, serviços e aplicativos.

Aproveitando os padrões baseados em Infraestrutura de Chave Pública (PKI) para autenticar e estabelecer confiança entre dispositivos IoT e serviços em nuvem, a integridade pode ser garantida, com a origem e criptografia de todos os dados transmitidos dentro do ecossistema.

Uma Plataforma de Identidade IOT fornecerá uma arquitetura de identidade digital desenvolvida especificamente para implementações de IoT e IIoT. Isso protege dispositivos IoT, dados e comunicações usando criptografia, autenticação e autorização. E, devido à natureza expansiva da IoT, a escalabilidade é crítica. A plataforma de identidade deve ser capaz de emitir milhares de certificados por segundo e centenas

de milhões de certificados todos os dias.

Criando um Ecossistema IoT Mais Seguro na Internet

As rodovias que dirigimos não são inerentemente seguras. Podemos criar maior proteção utilizando freios, cintos de segurança, airbags e os vários componentes do sistema de segurança do automóvel. Da mesma forma, a internet não é inerentemente segura, mas o tráfego que passa por ela ficar mais seguro através da implantação de medidas de segurança abrangentes, incluindo criptografia, identidades de dispositivo exclusivas, autenticação multifator, patches e atualizações regulares e a adoção de práticas seguras no uso de senha.

A GlobalSign fornece gerenciamento completo do ciclo de vida da identidade do dispositivo IoT, seja onde e quando o dispositivo for colocado em utilização.

Clique aqui para saber mais sobre como a GlobalSign pode ajudar a proteger sua infraestrutura de IoT.

Luiza Dias é diretora presidente da GlobalSign Brasil