ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL DEPUTADO ROBERTO MESQUITA

YASMIM RIBEIRO LIMA

DESAFIOS E SOLUÇÕES DE SEGURANÇA PARA DISPOSITIVOS LOT

GARANTIDO A SEGURANÇA EM DISPOSITIVOS LOT: RISCOS E SOLUÇÕES

GENERAL SAMPAIO, CEARÁ

2024

O que é?

É uma vasta rede de objetos físicos conectados. Esses dispositivos estão equipados com sensores, software e outras tecnologias. Dessa forma, eles trocam dados via Internet. Esse intercâmbio abrange desde aparelhos domésticos, como geladeiras e termostatos inteligentes, até ferramentas industriais avançadas e sistemas de monitoramento de saúde. Portanto, a IoT tem o potencial de revolucionar diversos setores, incluindo automação residencial, manufatura e saúde pública.

Qual sua importância?

Proteger dispositivos da internet e as redes às quais eles estão conectados contra ameaças e violações, por meio da proteção, identificação e monitoramento dos riscos e, ao mesmo tempo, ajudando a corrigir vulnerabilidades em uma variedade de dispositivos que possam apresentar risco de segurança para os seus negócios.

Principais ameaças

Entre as principais ameaças estão worms IoT, botnets para ataques DDoS, ransomware que bloqueia o acesso a dispositivos, ataques Man-in-the-Middle (MitM) e o sequestro de firmware por atualizações falsas. Por isso, esses riscos destacam a necessidade de medidas de segurança robustas para proteger usuários e dados.

Consequências da falta de segurança em IoT

A falta de segurança nos dispositivos IoT causa o crescimento de botnets usadas em ataques DDoS e outros ciberataques. Consequentemente, esses ataques interrompem serviços essenciais, causando prejuízos significativos. Por isso, a segurança da IoT é fundamental quando falamos das diversas ameaças cibernéticas e às práticas inseguras de usuários e organizações sem recursos ou conhecimentos adequados.

Como proteger os dispositivos de IoT

Utilize senhas fortes:

Criar senhas fortes é a base fundamental para garantir que seus dispositivos de IoT sejam protegidos e seguros. Uma senha forte é exclusiva, deve ter pelo menos 16 caracteres e incluir letras maiusculas e minúsculas, números e símbolos. Usar senhas exclusivas e fortes protegerá as contas dos seus dispositivos de IoT contra comprometimentos.

Proteja sua rede Wi-Fi:

Sua rede Wi-Fi é um gateway que cibercriminosos podem utilizar para acessar seus dispositivos de IoT. Se um cibercriminoso obter acesso à sua rede, ele poderá explorar qualquer dispositivo conectado e toda a rede Wi-Fi. Esse risco pode ser minimizado alterando a senha padrão do seu roteador Wi-Fi para uma que seja forte e exclusiva. Certifique-se de também alterar o nome da rede padrão da sua rede Wi-Fi para uma nova que não inclua informações pessoais, como seu primeiro nome ou sobrenome. Uma medida adicional que você pode tomar para proteger sua rede Wi-Fi é ativar a criptografia por meio das configurações de administrador do seu roteador Wi-Fi.

Desconecte seu dispositivos de IoT quando não estiverem em uso:

Reduzir sua superfície de ataque pode ser feito simplesmente desconectando os dispositivos de IoT quando você não os estiver usando. Isso reduzirá o risco de ataques porque você elimina esse dispositivo como um caminho para obter acesso à sua rede.

Ajuste suas configurações do seu dispositivo IoT:

Também é importante avaliar suas configurações de dispositivos de IoT e desativar quaisquer recursos e serviços que você não esteja usando. Muitas vezes, esses dispositivos podem ter uma variedade de recursos que podem não ser necessários ou relevantes para você. Essas funcionalidades ociosas apresentam um risco de segurança cibernética porque criam uma superfície de ataque maior.