ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL DEPUTADO ROBERTO MESQUITA

CLARISSA VITÓRIA RODRIGUES SIQUEIRA

DESAFIOS E SOLUÇÕES DE SEGURANÇA PARA DISPOSITIVO LOT:

Riscos e Mitigações em Ambientes Conectados

GENERAL SAMPAIO-CEARÁ
2024

INTRODUÇÃO

A Internet das Coisas (IoT) está transformando a maneira como interagimos com o mundo, conectando uma vasta gama de dispositivos que antes não estavam ligados à internet. Desde eletrodomésticos inteligentes até dispositivos de monitoramento de saúde, a IoT está presente em diversos aspectos de nossas vidas. No entanto, essa conectividade traz consigo desafios significativos de segurança. Este trabalho explora os principais riscos associados aos dispositivos IoT e as estratégias de mitigação para garantir um ambiente conectado seguro.

Principais Riscos de Segurança em Dispositivos IoT

Vulnerabilidades de Software: Muitos dispositivos IoT são lançados com falhas de segurança que podem ser exploradas por atacantes.
Falta de Atualizações: A ausência de atualizações regulares de software e firmware deixa os dispositivos expostos a novas ameaças.
Autenticação Fraca: Senhas padrão e métodos de autenticação inadequados facilitam o acesso não autorizado.
Privacidade de Dados: A coleta e transmissão de dados pessoais sem a devida proteção pode levar a violações de privacidade.

Soluções e Mitigações

Criptografia de Dados: Implementar criptografia forte para proteger os dados transmitidos e armazenados.
Autenticação Robusta: Utilizar métodos de autenticação multifator para garantir que apenas usuários autorizados possam acessar os dispositivos.
Atualizações Regulares: Garantir que os dispositivos recebam atualizações de software e firmware para corrigir vulnerabilidades conhecidas.
Segmentação de Rede: Implementar firewalls e segmentação de rede para limitar o acesso aos dispositivos IoT e proteger contra ataques cibernéticos.

CONCLUSÃO

A segurança em dispositivos IoT é um desafio contínuo que requer uma abordagem multifacetada. Ao implementar práticas robustas de segurança, como criptografia, autenticação forte, atualizações regulares e segmentação de rede, é possível mitigar os riscos e garantir a integridade e confidencialidade dos dados em um mundo cada vez mais conectado. A colaboração entre fabricantes, desenvolvedores e usuários é essencial para criar um ecossistema IoT seguro e confiável.