Segurança em Redes IoT – TP546

Nome: Denise Silva Figueiredo

Introdução

Dispositivos de Internet das Coisas (IoT) são instrumentos computadorizados conectados à internet, tendo como exemplo câmeras de segurança em rede, refrigeradores inteligentes, e automóveis com recursos Wi-Fi. O processo para proteger esses dispositivos é conhecido como segurança da IoT, que tem garantia em fazer com que eles não introduzam ameaças.

Sabemos que estando conectada a internet, provavelmente enfrentará ataques em qualquer momento, podendo tentar comprometer remotamente dispositivos de IoT usando diversos métodos, desde roubos de credenciais até explorações de vulnerabilidades, roubando dados e até mesmo tentando comprometer o restante da rede conectada.

A segurança da IoT pode ser tentadora porque muitos dispositivos de IoT não são construídos com segurança capaz de impedir esses invasores, normalmente o foco do fabricante está em recursos e usabilidade, em vez de segurança, fazendo com que os equipamentos cheguem ao mercado rapidamente.

Como esses dispositivos de IoT lidam com dados pessoas e operam em ambientes como casas, empresas e até sistemas industriais, implementar medidas de segurança é indispensável.

Algumas práticas eficazes para melhorar a segurança em redes IoT são:

- Autenticação e controle de acesso, contendo senhas fortes para cada dispositivo, evitando usar senhas padrões; autenticação multi-fator, quando possível para dificultar o acesso a invasores e controle para acessos, definindo permissões claras para diferentes tipos de usuários e dispositivos de rede.
- Criptografia de dados, como em trânsito utilizando protocolos como TLS (Transport Layer Security) para proteger dados transmitidos entre dispositivos e servidores e dados em repouso, armazenando de forma criptografada para evitar o acesso não autorizado em caso de violação da segurança.
- Segmentação da rede, tendo uma rede fragmentada, colocando dispositivos em rede separada da rede principal para minimizar os riscos de propagação de ataque e firewall para monitorar e controlar o tráfego de rede entre dispositivos IoT e outras partes da rede.
- Monitoramento e detecção de ameaças, com o continuo acompanhando o tráfego e o sistemas de detecção de intrusões (IDS) para detectar comportamentos anômalos possíveis tentativas de invasão.
- Segurança física dos dispositivos, utilizando a proteção física garantindo que os dispositivos estejam em locais seguros e desativação de portas não necessárias que faz o processo de desativar as portas que não são necessárias e minimize pontos de entrada física que podem ser explorados.
- Política de privacidade e proteção de dados, configura dispositivos para coletar e armazenar apenas os dados essenciais e anonimização e pseudonimização protegendo a privacidade dos usuários.
- Educação e conscientização treinando os usuários sobre as práticas de segurança e conscientização dos riscos.
- Uso de protocolo e padrões de segurança, como protocolo específicos para IoT, como MQTT com TSL, CoAP com DTLS e IEEE 802.1X, certificações de segurança seguindo normas e certificações de segurança conhecidas.

- Avaliação e gestão de riscos fazendo analise regularmente os riscos de segurança associados aos dispositivos IoT e fazendo ajustes necessários para proteção, e o plano de recuperação de desastres, caso ocorra uma invasão.

Essas técnicas são muito importantes para combater ameaças e garantir proteção da rede contra vulnerabilidades, sendo assim é importante que as estratégias de segurança sempre sejam revisadas e atualizadas.

As redes IoT trazem vantagens, mas apresentam desafios significativos para a segurança. Devido a conexão e muitas vezes distribuída nos dispositivos, além de limitações de hardware e software, que tendem a tornar alvos pra cibercriminosos, assim encontra-se alguns problemas para a segurança em redes IoT, sendo elas:

- Falta de atualizações e suporte de segurança, muitos dispositivos não recebem atualizações de segurança regulares, deixando vulnerável para serem invadidas, alguns dispositivos também são descontinuados e o suporte e atualizações de segurança são encerrados, tornando também suscetíveis a ameaças.
- Credenciais fracas e padrões de segurança inadequados, com senhas padrão fáceis e os usuários não alteram, mecanismos de autenticação fracos ou inexistentes.
- Criptografia insuficiente, com dados em texto simples e usando uma implementação fraca de criptografia.
- Falta de padrões de segurança universais contendo inconsistência entre fabricantes, não contendo um padrão universal de segurança, resultando em diferentes níveis de proteção e compatibilidade e até mesmo protocolos de comunicação proprietários, que são menos seguros e mais difíceis de integrar com sistemas de segurança existentes.
- Exposição a ataques de malware específicos que aproveitam a vulnerabilidade e limitações do aparelho.
- Falta de visibilidade e monitoramento, em muitas redes não há evidência sobre os equipamentos conectados, dificultando a detecção de atividades suspeitas e sem monitoramento faz com que não consiga perceber o invasor rapidamente, permitindo que o ataque prolongue.
- Falhas de compatibilidade e riscos de integração podem expor toda a rede.
- Ameaças a privacidade, dispositivos que coletam dados a mais do que necessário aumentando o risco de vazamento de informações pessoais, comprometendo o usuário acessar.
- Ataques físicos aos dispositivos, quando instalados em local publico pode facilmente ser manipulados, permitindo ataques modificando o dispositivo ou coletando informações existentes nele, até mesmo clonar.
- Desafios de escalabilidade e gestão de dispositivos, fazendo com que de acordo com o crescimento de dispositivos IoT, o gerenciamento e proteção se torna cada vez mais difícil fazendo com que alguma vulnerabilidade tenha mais chances e possibilitando a dificuldade de se perceber qualquer tipo de ataque.
- Ataques de negação de serviço DoS e DDoS, ataques DDoS sobrecarrega os servidores com tráfego causando interrupções no serviço e os ataques DoS podem fazer com que o dispositivo fique offline ou parem de funcionar, interrompendo serviços vulneráveis.

- Vulnerabilidade do software e firmware, quando o firmware não é atualizado, deixa o dispositivo exposto a ameaças e as configurações padra ou incorretas de fábrica podem expor os equipamentos, principalmente quando o usuário não faz ajustes de segurança.

É primordial que com esses problemas, os fabricantes, desenvolvedores e usuários estejam atentos e implemente práticas de segurança, com atualizações frequentes, autenticação forte, segmentação da rede e monitoramento constante, para tentar enfrentar possíveis ameaças.

Ataque de falsificação de comandos acontece quando o invasor encontra uma interface ou aplicação que aceita comandos, como uma interface web para controle do dispositivo, o atacante insere este comando em um campo de entrada, aproveitando da falta de validação. Com a falta de validação ou ser filtrado adequadamente o comando, o dispositivo executa, permitindo que o invasor obtenha acesso ao sistema ou realize ações não autorizadas. Dependendo do comando pode incluir, acesso aos sistemas de arquivos, modificações de configurações, transferências de dados e instalação de malware.

Este tipo de ataque pode ter consequências como acesso ao sistema operacional e obter controle sobre o dispositivo, modificando dados, alterando configurações de segurança ou roubar informações. O invasor pode instalar backdoors ou outro malware, que transforma o dispositivo em um ponto de entrada para outros ataques, podendo também deletar arquivos, comprometendo a funcionabilidade do arquivo.

Para evitar os riscos de ataque de injeção de comando é importante algumas práticas como:

1- Sempre filtrar e validar a entrada de usuários para impedir caracteres especiais de comandos inesperados;

2- Utilizar API’s e comandos que não permitem execução de comandos arbitrários. Evitando a execução destes comandos do sistema de entrada de usuário;

3- Configurar o dispositivo para executar comandos com o mínimo de privilégios necessários, limitando o que pode ser acessado ou modificado;

4- Manter o firmware e o software dos dispositivos IoT sempre atualizados para garantir que a vulnerabilidade seja corrigida;

5- Utilização de ferramentas como firewalls de aplicações web (WAF) e sistemas de detecção de intrusões (IDS) podem ajudar a monitoração e bloqueio de injeção de comandos.

Mas caso este tipo de ataque aconteça é necessária uma ação imediata, desconectando o dispositivo IoT da rede para interromper o acesso remoto do atacante, impedindo que o malware se espalhe. Caso o malware já tenha se espalhado, considere isolar outros dispositivos IoT ou a rede evitando que os dispositivos sejam comprometidos. Caso o invasor tenha usado um IP específico é necessário o bloqueio no firewall para impedir novas conexão. Importante fazer uma revisão dos logs do dispositivo e da rede para identificar o que foi feito e caso tenha sido feito download ou execução de arquivos suspeitos, envie-os para análise de malware em uma ferramenta de segurança. Se possível, restaure o dispositivo para um estado seguro, removendo qualquer malware, comandos ou scripts que foram introduzidos. Se houver uma função de garantir que o dispositivo volte as configurações originais, removendo qualquer modificação do invasor.

Indispensável verificar se há uma atualização de firmware disponível, aplique-a para corrigir qualquer vulnerabilidade que o invasor possa ter explorado. É necessário redefinir senhas fracas e ativar autenticação multifatorial, revisando o código de aplicativos e interface que recebem entrada de usuário e implementar uma validação e filtragem para evitar a execução de comandos, colocando o dispositivo em uma rede isolada para limitar o impacto.

Fazer o monitoramento contínuo e manter registros detalhados das atividades do dispositivo IoT para referência futura e como medida de prevenção. Notificar equipes de segurança, possíveis vazamento de dados. Importante sempre revisar e atualizar essas políticas de segurança, avaliando e tendo como plano estratégia para ataques futuros.