Segurança da informação e proteção de dados

temos que analisar as principais ameaças ao nosso sistema: a segurança é o ponto mais importante da nossa cidade, pois os cibercriminosos podem se aproveitar de falhas na segurança para roubar dados sensíveis e atrapalhar na comunicação de diversos dispositivos principalmente na coleta de dados de sensores IOT.

1. **Principais ameaças e vulnerabilidades**.

    - **Ataques DDOS:** Como um dos principais meio de ataques a grandes sistemas de dados temos o DDOS, ele visa sobrecarregar a infraestrutura de redes, resultando em travamentos e até quedas na rede de tráfego afetando sistemas de semáforos, controle de tráfego e sensores de segurança.

    - **Invasão de dispositivos IOT:** muitos dispositivos IOT tem sua segurança fraca, oque pode ser alvo de hacker, caso vários dispositivos forem infectados com algum malware eles podem ser usados como botnets e usados para manipular sensores ou coletas de dados pessoais.

    - **Protocolos de comunicação inseguros:** Muitas vezes, a comunicação entre dispositivos IoT é realizada usando protocolos pouco seguros, como HTTP sem criptografia, que pode ser interceptada por atacantes, protocolos como MQTT ou CoAP, comuns em IoT, também podem ser alvos de exploração**.**

    - **Ataque a bases de dados:** as bases de dados são grandes alvos pois armazenam grandes quantidades de informações sensíveis e de grande valor comercial, se mal protegidas podem vazar esses dados e causar um dano significativo a privacidade dos cidadãos.

2. **Como a engenharia social pode ser uma ameaça à segurança.**

A engenharia social é uma técnica de manipulação psicológica usada para ter acesso a informações confidenciais, sistemas ou recursos. Em uma cidade inteligente isso seria extremamente grave pois as pessoas são facilmente manipuladas. Alguns exemplos de técnicas de engenharia social são:

- **Phishing**: essa técnica envolve o envio de e-mails falsos disfarçados de e-mails de empresas reais como bancos exigindo informações sensíveis ou credenciais para acessar suas contas.

- **Pretexting**: O atacante se faz passar por alguém de confiança para obter informações confidenciais.

Práticas de prevenções

- **Treinamento e conscientização**: Funcionários da cidade inteligente devem ser treinados regularmente para reconhecer técnicas de engenharia social, como phishing e pretexting.

- **Autenticação Forte**: Usar autenticação multifatorial (MFA) sempre que possível, para garantir que apenas pessoas autorizadas tenham acesso a sistemas sensíveis e trocar de senha regularmente.

3. **Proteção e criptografia**

A proteção de dados de uma cidade inteligente deve ser feita com diversos métodos sendo o principal deles a criptografia a melhor técnica para manter a segurança das informações e o armazenamento seguro de dados.

- **Criptografia de dados em trânsito:** A utilização de SSL/TLS garante que os dados transmitidos entre dispositivos IoT e os servidores centrais sejam criptografados isso impede que atacantes interceptem ou alterem os dados em trânsito, os protocolos MQTT e CoAP devem ser configurados para funcionar com TLS para garantir a segurança na troca de mensagens entre dispositivos.

- **criptografias de dados em repouso:** para criptografar esses dados que estão armazenados deve ser utilizado a criptografia AES que criptografa arquivos na armazenados em servidores e bancos de dados para que o hacker mesmo com acesso físico ao hardware não consiga ter acesso aos dados. Além disso técnicas de tokenização ou hashing podem ser usadas para proteger informações sensíveis, como números de identificação de cidadãos ou dados financeiros.

- **Criptografia de dados IOT:** para garantir a segurança das IOTS nosso calcanhar de Aquiles deve-se usar secure boot para ele inicializar com firmware autentificado, prevenindo que malwares sejam carregados no dispositivo, as chaves Públicas e Privadas seriam para implementam criptografia assimétrica, onde cada dispositivo IoT tem um par de chaves públicas e privadas. A chave pública é usada para criptografar os dados e a chave privada é usada para descriptografá-los, garantindo a integridade e confidencialidade da comunicação e para garantir a integridade dos dados transmitidos entre dispositivos IoT, pode-se usar assinaturas digitais

4. **Normas de Segurança e Políticas de Gerenciamento de Dados**

Existem diversas normas e regulamentos que orientam a segurança da informação e a proteção de dados. Algumas das mais relevantes para uma cidade inteligente incluem**:**

- **Regulamentos e normas:** dentro de regulamentos e normas temos a lei LGPD leis que impõem regras rigorosas sobre como os dados devem ser coletados, armazenados, processados e compartilhados. Também temos a lei ISO/IEC 27001 que define requisitos para um sistema de gestão de segurança e pôr fim a NIST Cybersecurity Framework fornece um conjunto de melhores práticas e diretrizes para a gestão de riscos cibernéticos.

- **Políticas de gerenciamento de dados:** devemos definir claramente quais dados pessoais vamos armazenar, implementar políticas de backup e restauração de dados para caso esses arquivos sejam perdidos, estabelecer procedimentos de monitoramento em tempo real para detectar atividades suspeitas.