PROJETO A3
UC – SISTEMAS COMPUTACIONAIS E SEGURANÇA

Alunos

Arthur Carvalho – 825119250

Fabio Marano – 825111150

Leonardo Ferreira – 825124892

Lucas Garcia – 825145166

Matheus Fraga – 82425021

Matheus Fidelis – 825144599

CIBERSEGURANÇA EM INFRAESTRUTURAS CRÍTICAS DE CIDADES INTELIGENTES COM FOCO EM IOT

- A crescente integração de dispositivos IoT nas infraestruturas críticas das cidades inteligentes amplia a eficiência e a automação, mas também eleva os riscos de segurança cibernética. A proteção desses sistemas é essencial para garantir a segurança, a confiabilidade e a continuidade dos serviços urbanos.

PESQUISA E LEVANTAMENTO DE DADOS

- Com o avanço das Cidades Inteligentes, sistemas críticos passaram a ser conectados via IoT, ampliando as possibilidades de inovação, mas também aumentando a superfície de ataque.

- Problema: Dispositivos IoT podem ser alvos de ataques que comprometem a infraestrutura urbana.

ESTUDOS DE CASOS

- 1. Ataque ao sistema de água na Flórida (2021): tentativa de envenenamento da água.
- 2. Botnet Mirai (2016): ataque massivo com dispositivos IoT comprometidos.

VANTAGENS E DESVANTAGENS

- Vantagens:
- - Eficiência
- - Automatização
- - Redução de custos

- Desvantagens:
- - Vulnerabilidades
- - Falta de padrões
- - Dificuldade de atualização
- - Risco de falhas em serviços essenciais

PROPOSTA DA SOLUÇÃO

- SafeCity IoT Shield – Sistema de Monitoramento e Prevenção de Ameaças Cibernéticas em Infraestruturas IoT Urbanas

COMPONENTES DA SOLUÇÃO

- 1. Sensores e Agentes IoT de Segurança
- 2. Plataforma de Monitoramento Centralizada
- 3. Sistema de Detecção e Prevenção de Intrusões (IDPS)
- 4. Mecanismos de Autenticação e Criptografia
- 5. Atualização Automática de Firmware

FLUXO DE FUNCIONAMENTO

- 1. Detecção de anomalia
- 2. Alerta ao IDPS
- 3. Análise e ação: bloqueio, isolamento ou notificação
- 4. Execução da ação
- 5. Geração de relatório

IMPACTOS DA SOLUÇÃO

- Tecnológico: fortalece segurança IoT.
- Econômico: reduz prejuízos.
- Social: protege cidadãos.
- Ambiental: evita desperdícios.

VIABILIDADE TÉCNICA

- Tecnologias maduras: machine learning, protocolos de segurança.
- Desafios: compatibilidade entre fabricantes.
- Necessidade de capacitação em cibersegurança IoT.

CONCLUSÃO

Com o avanço das tecnologias de Internet das Coisas (IoT), as cidades inteligentes passaram a incorporar dispositivos e sistemas conectados para melhorar a eficiência dos serviços públicos, como transporte, energia, segurança e meio ambiente. No entanto, essa crescente conectividade também amplia a superfície de ataque cibernético, colocando em risco infraestruturas críticas que sustentam o funcionamento das cidades.

Este projeto propõe o desenvolvimento do **"SafeCity IoT Shield"**, uma solução inovadora voltada para o monitoramento e prevenção de ameaças cibernéticas em dispositivos e sistemas IoT implantados em ambientes urbanos. A proposta inclui o uso de sensores de segurança embarcados, plataformas de monitoramento centralizadas, sistemas de detecção e prevenção de intrusões (IDPS), além de mecanismos robustos de autenticação e criptografia.

REFERÊNCIAS

- - ENISA
- - OWASP
- - Gartner
- - NIST
- - Relatórios de casos: Flórida (2021), Botnet Mirai (2016)