

Nome: Felipe Morais Carrapeiro RM-84507

Explicação sobre a solução desenvolvida

Esta solução visa proporcionar segurança para os familiares idosos das pessoas, e conseqüentemente tranquilizar os familiares responsáveis.

A Solução em si se trata de uma forma de monitoramento de possíveis perigos residenciais que uma pessoa idosa possa presenciar, sendo eles: vazamento de gás, incêndio e queda.

Funcionamento

O idoso possuirá um Arduino em sua residência próximo de possíveis ocorrências de vazamento de gás ou incêndio, este Arduino possuirá uma configuração para detectar as ocorrências citadas. Para a detecção de queda o idoso deverá usar uma pulseira com micro-sensores que identificarão movimentações bruscas. Ao ser identificado alguma destas ocorrências, uma ligação será feita para o número de telefone cadastrado informando qual possível risco o idoso sofreu.

Para o funcionamento de todas estas funções, existirá um WebApp, onde o usuário responsável pelo idoso deverá realizar um cadastro informando email, senha e número de telefone, para assim possuímos as informações necessárias para notificar o mesmo. O usuário também poderá escolher dentre uma ou mais formas de notificação, sendo por e-mail, sms ou ligação. Estes meios também poderão possuir mais de uma ponta final para serem notificadas, podendo ser de diferentes e-mails e números telefônicos.

Um protótipo desenvolvido já pode ser acessado: <http://front-faculdade.s3-website-sa-east-1.amazonaws.com/home>

Segurança

Esta aplicação não será focada apenas em garantir a segurança física do idoso, mas também em proteger os dados sensíveis do usuário contra ameaças cibernéticas. A solução incluirá uma série de medidas de segurança cibernética conforme as diretrizes do OWASP Top 10 sendo elas:

1. Avaliação de Risco:

Identificar possíveis riscos e vulnerabilidades no sistema de monitoramento.

Priorizar áreas críticas que exigem proteção adicional evitando ameaças como injeção de código, acesso não autorizado, entre outros.

2. Práticas de Autenticação Segura:

Será implementado formas de autenticação, sendo elas: bloqueio de contas após várias tentativas de login fracassadas e autenticação de dois fatores necessitando informar códigos enviados tanto nos e-mails quanto números telefônicos cadastrados.

Armazenamento seguro das credenciais informadas para assim garantir a proteção das informações de login dos usuários, utilizando o formato de criptografia 'hash and salt'.

3. Proteção das Comunicações:

Será utilizado alguns protocolos de criptografia, como SSL/TLS, para realizar a proteção das comunicações entre dispositivos e servidores.

Prevenção de possíveis interceptações de dados sensíveis durante a transmissão.

4. Validação de Entrada de Dados:

Será realizado validações das informações preenchidas tanto para evitar entrada de dados maliciosos quanto para garantir que os dados informados são reais enviando e-mails/sms de confirmação para o uso devido da aplicação.

5. Controle de Acesso Adequado:

Será implementado um modelo de controle de acesso baseado em permissionamento de funções, para ter a garantia de que os usuários possuam acesso somente às funcionalidades e dados necessários para suas ações.

6. Manutenção de Software Atualizada:

Possuirá a garantia de que todos os módulos de software estejam sempre atualizados com as últimas atualizações de segurança e patches.

7. Monitoramento e Registro de Atividades:

Serão implementados mecanismos de monitoramento que registrem e alertem sobre qualquer atividade suspeita.

8. Testes de Segurança Regulares:

Serão realizados testes de invasão e avaliações de segurança regularizadas para identificar e corrigir vulnerabilidades.

9. Implementação de firewall:

Será implementado um firewall de rede entre o backend, as interfaces do frontend e o dispositivo Arduino.

Algumas regras serão definidas para permitir apenas o tráfego necessário para a operação do sistema, bloqueando todo tráfego não autorizado.

Conclusão:

Seguindo as diretrizes do OWASP Top 10 e implementando as medidas de segurança cibernética desde o início do desenvolvimento da aplicação, será construído uma base confiável para oferecer uma proteção abrangente aos nossos usuários.