UNIFEOB
ESCOLA DE NEGÓCIOS

2023

PROJETO DE CONSULTORIA EMPRESARIAL

UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

CHATBOT SEGURANÇA DA INFORMAÇÃO

VARGEM GRANDE DO SUL, SP

NOVEMBRO 2023

UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

CHATBOT SEGURANÇA DA INFORMAÇÃO

MÓDULO - Inteligência Artificial

Inteligência Artificial – Prof. Rodrigo Marudi de Oliveira

Segurança em Sistema Computacionais - Prof. Nivaldo de Andrade

Estudantes:

Estudante Pedro Barrese, RA 1012022201137

Estudante Tatiane Soares de Oliveira, RA 1012023100036

VARGEM GRANDE DO SUL, SP

NOVEMBRO, 2023

SUMÁRIO

1 INTRODUÇÃO

No vasto panorama da cibersegurança, mesmo soluções simples podem desempenhar um papel crucial na proteção dos usuários contra ameaças digitais em constante evolução. O projeto em foco, um chatbot dedicado a fornecer dicas práticas para se resguardar contra vírus, phishing e outras vulnerabilidades, representa uma abordagem descomplicada, porém fundamental, para promover a consciência e a segurança cibernética.

Este chatbot, desenvolvido utilizando Python, busca simplificar um aspecto cada vez mais complexo do mundo digital: a proteção dos dados e da privacidade dos usuários. Oferecendo orientações acessíveis e diretas, visa capacitar os indivíduos a adotarem medidas simples, porém eficazes, para protegerem-se contra potenciais ameaças.

Embora a solução proposta possa parecer modesta em sua implementação, sua relevância não deve ser subestimada. Em um ecossistema digital onde a sofisticação das ameaças muitas vezes sobrepõe a compreensão dos usuários, o chatbot assume um papel valioso ao democratizar o acesso a informações e práticas que fortalecem a segurança pessoal online.

Este documento resume não apenas o desenvolvimento técnico do chatbot, mas também a essência de sua proposta: tornar a segurança da informação compreensível e aplicável para todos. A simplicidade desta solução não diminui sua importância, mas, pelo contrário, ressalta a necessidade urgente de abordagens acessíveis na batalha contínua contra ameaças digitais.

2 DESCRIÇÃO DA EMPRESA

Empresa: CyberSecTips Ltda.

Razão Social: CyberSecTips Ltda.

CNPJ: 123.456.789/0001-00

Endereço: Rua da Inovação, 123 - Cidade Cyber, Estado Techland - CEP: 01234-567

A CyberSecTips Ltda. é uma empresa especializada em soluções de segurança da informação. Nosso foco principal está na conscientização e educação em cibersegurança, oferecendo ferramentas e orientações para indivíduos e empresas protegerem-se contra ameaças digitais.

Atuando em um mercado altamente dinâmico e tecnológico, a CyberSecTips Ltda. está inserida no setor de segurança cibernética, um segmento de vital importância no cenário contemporâneo. Diante do aumento exponencial de ameaças digitais, desde vírus até ataques sofisticados de phishing, a demanda por soluções acessíveis e eficazes de segurança da informação tem crescido significativamente.

Nossa empresa oferece um portfólio diversificado de produtos e serviços, com destaque para:

Nosso principal produto é um chatbot inovador desenvolvido em Python, projetado para fornecer dicas práticas e relevantes para proteção contra vírus, phishing e outras vulnerabilidades cibernéticas. Esse chatbot busca simplificar a compreensão e aplicação de práticas de segurança para usuários individuais e corporativos.

Além disso, oferecemos workshops e treinamentos personalizados, adaptados para atender às necessidades específicas de cada cliente. Essas sessões abrangem desde noções básicas de segurança cibernética até estratégias avançadas de proteção de dados.

Nossa equipe de especialistas em segurança da informação também fornece serviços de consultoria para empresas que buscam aprimorar suas estratégias de proteção de dados, implementando protocolos robustos e garantindo conformidade com os padrões de segurança.

.

3 PROJETO DE CONSULTORIA EMPRESARIAL

Histórico da Empresa:

A CyberSecTips Ltda. foi fundada em 2015 por um grupo de especialistas em segurança da informação apaixonados por simplificar a proteção digital. Desde então, temos nos destacado no mercado por oferecer soluções inovadoras e acessíveis em cibersegurança. Nosso compromisso com a proteção dos usuários e empresas tem sido o núcleo de nossa jornada, impulsionando nosso crescimento e reconhecimento no setor.

Ramo de Atuação e Propósito:

Atuamos no ramo da segurança da informação, com a missão de tornar a proteção digital acessível e compreensível para todos. Nossa visão é criar um ambiente digital seguro, onde indivíduos e organizações possam aproveitar ao máximo as tecnologias emergentes sem preocupações com ameaças cibernéticas.

Valores da Empresa:

-Acessibilidade: Acreditamos na democratização da segurança cibernética, tornando-a acessível a todos.

-Inovação: Buscamos constantemente novas maneiras de simplificar a proteção digital por meio da inovação tecnológica.

-Transparência: Valorizamos a transparência em todas as interações, fornecendo informações claras e precisas sobre segurança da informação.

-Compromisso com a Segurança: Comprometemo-nos em garantir a proteção dos dados e a privacidade dos usuários em todas as nossas soluções.

Desafios e Motivação para Consultoria:

Os principais desafios que enfrentamos como empresa estão alinhados com a constante evolução das ameaças cibernéticas. Com o surgimento de novos métodos e técnicas por parte dos invasores digitais, percebemos a necessidade de aprimorar continuamente nossas soluções para oferecer proteção eficaz.

A busca por consultoria em inteligência artificial e segurança em sistemas computacionais foi motivada pela crescente complexidade das ameaças digitais e pela demanda por soluções mais robustas. Reconhecemos a importância de integrar técnicas avançadas de IA em nossa infraestrutura de TI para melhorar a detecção proativa de ameaças e fortalecer nossos sistemas contra possíveis vulnerabilidades.

.

3.1 INTELIGÊNCIA ARTIFICIAL

Visão Geral da Inteligência Artificial:

A Inteligência Artificial (IA) é um ramo da ciência da computação que se concentra no desenvolvimento de sistemas capazes de realizar tarefas que normalmente requerem inteligência humana. Esses sistemas são projetados para aprender, raciocinar, perceber, entender e tomar decisões de forma autônoma.

Relevância da Inteligência Artificial na Atualidade:

A relevância da IA na atualidade é indiscutível, permeando diversas esferas da nossa vida cotidiana. Ela impulsiona avanços significativos em áreas como saúde, finanças, transporte, entretenimento e, especialmente, segurança da informação. Sua capacidade de analisar grandes volumes de dados, identificar padrões e tomar decisões rápidas a torna uma ferramenta essencial para lidar com a complexidade dos ambientes digitais contemporâneos.

Importância da Integração da IA no Contexto do Projeto:

A integração da IA no contexto do projeto é crucial para aprimorar a eficiência e a eficácia das soluções de segurança da informação oferecidas pelo chatbot. A IA pode potencializar a capacidade do chatbot de identificar e responder a ameaças em tempo real, oferecer recomendações personalizadas e adaptar-se continuamente às novas estratégias de ataque, garantindo assim uma proteção mais abrangente e proativa aos usuários.

Ao utilizar algoritmos de IA, como aprendizado de máquina e processamento de linguagem natural, o chatbot pode aperfeiçoar suas capacidades de reconhecimento de padrões, detecção de comportamentos suspeitos e personalização das dicas de segurança, fornecendo um serviço mais refinado e adaptado às necessidades específicas dos usuários.

3.1.1 Introdução à Aplicação da IA

Aplicação de Detecção de Anomalias:

Nos sistemas de segurança da informação, a detecção de anomalias é fundamental para identificar comportamentos ou eventos incomuns que podem indicar atividades maliciosas ou ataques cibernéticos. Algoritmos de Inteligência Artificial, como os baseados em aprendizado de máquina, têm sido amplamente empregados para essa finalidade.

Exemplo Prático de Uso:

Um exemplo real dessa aplicação está na detecção de fraudes em transações financeiras. Instituições financeiras utilizam algoritmos de IA para analisar padrões de comportamento de transações, identificar desvios em relação ao comportamento normal do usuário e, assim, detectar possíveis atividades fraudulentas, como o uso não autorizado de cartões de crédito ou débito.

Esses algoritmos aprendem com grandes volumes de dados históricos, identificam padrões de transações legítimas e, quando detectam discrepâncias significativas, acionam alertas para investigação humana ou bloqueiam automaticamente a transação suspeita, ajudando a evitar fraudes financeiras.

Relevância para o Projeto de Segurança da Informação:

No contexto do projeto do chatbot de segurança da informação, essa aplicação de detecção de anomalias pode ser relevante para aprimorar a capacidade do chatbot de reconhecer comportamentos suspeitos nos padrões de uso, identificando, por exemplo, tentativas de acesso não autorizado, atividades de phishing ou uso atípico de dados,

permitindo uma resposta proativa e personalizada para orientar os usuários sobre possíveis ameaças.

3.1.2 Implementação e Técnicas Utilizadas

Técnicas Específicas de IA e Ferramentas Relevantes:

-Redes Neurais Convolucionais (CNNs): As CNNs são modelos de aprendizado profundo (deep learning) frequentemente utilizados para análise de imagens. No contexto de segurança da informação, podem ser empregadas na detecção de padrões visuais em ataques cibernéticos ou na análise de logs visuais.

- Redes Multicamada (MLPs): As MLPs são redes neurais artificiais com várias camadas de neurônios. Podem ser empregadas para classificação e identificação de padrões em dados não estruturados, como textos ou comportamentos de usuários.

- Perceptrons: São modelos básicos de redes neurais que podem ser utilizados para tarefas simples de classificação binária.

- Linguagens e Ferramentas: Para implementar essas técnicas, linguagens como Python são amplamente utilizadas, principalmente com bibliotecas como TensorFlow e Keras para desenvolvimento de redes neurais. Ferramentas como o Teachable Machine do Google podem ser úteis para treinar modelos simples de aprendizado de máquina com imagens ou sons.

Relevância da Inteligência Artificial para o Projeto:

A escolha da disciplina de Inteligência Artificial é fundamental para o projeto de segurança da informação, pois oferece técnicas poderosas para aprimorar a eficácia do chatbot. A IA pode melhorar a capacidade do chatbot de identificar e responder a possíveis ameaças de maneira mais precisa e rápida, proporcionando orientações de segurança personalizadas aos usuários.

Ao integrar técnicas como CNNs para análise visual de possíveis ameaças, MLPs para compreensão e classificação de padrões de comportamento, e até mesmo Perceptrons para identificação de ameaças simples, o chatbot pode oferecer um nível mais avançado de detecção e aconselhamento em segurança da informação.

A utilização de linguagens como Python e suas estruturas de dados relevantes, em conjunto com ferramentas como o Teachable Machine do Google, oferece uma base sólida para a implementação e treinamento desses modelos de IA, permitindo a criação de um chatbot mais inteligente e adaptável.

A Inteligência Artificial, neste contexto, não só otimiza a detecção de ameaças, mas também possibilita uma resposta mais ágil e personalizada aos usuários, contribuindo significativamente para a eficácia do projeto ao oferecer um serviço mais seguro e adaptado às necessidades específicas dos usuários.

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

Importância da Segurança em Sistemas Computacionais:

A Segurança em Sistemas Computacionais é crucial para proteger dados, informações sensíveis e a infraestrutura digital de uma empresa contra ameaças cibernéticas. Os conceitos aprendidos em sala de aula proporcionam a base para compreender e implementar estratégias robustas de segurança, incluindo autenticação, criptografia, controle de acesso e detecção/prevenção de intrusões.

Aplicação dos Conceitos Aprendidos:

Na empresa CyberSecTips Ltda., os conceitos de segurança em sistemas computacionais foram aplicados de diversas maneiras. A implementação de protocolos de criptografia para proteger dados sensíveis, a configuração de firewalls para controlar o tráfego de rede e a utilização de autenticação multifatorial para garantir a identidade dos usuários foram algumas das estratégias adotadas.

Os princípios de segurança em programação também foram aplicados no desenvolvimento do chatbot de segurança da informação. A validação de entrada de dados, a

prevenção de injeção de código e a implementação de práticas de segurança no armazenamento e processamento de informações foram considerações cruciais durante o desenvolvimento.

Desafios Enfrentados na Implementação:

Durante a implementação desses conceitos, alguns desafios foram enfrentados. A complexidade de integrar camadas adicionais de segurança sem comprometer a usabilidade e a performance do chatbot foi um dos principais desafios. Equilibrar a proteção dos dados sem prejudicar a experiência do usuário tornou-se um objetivo desafiador.

Além disso, a constante evolução das ameaças cibernéticas demandou uma abordagem proativa na atualização e aprimoramento contínuo dos protocolos de segurança implementados. Garantir que os sistemas estivessem protegidos contra as mais recentes ameaças representou um desafio dinâmico ao longo do processo de implementação..

3.2.1 Conceitos e Implementação de Segurança

Com base nos tópicos "Conceitos de segurança lógica física" e "Conceito e Valor da Informação", os estudantes devem:

- Definir: Comecem por definir brevemente estes conceitos para contextualizar o leitor.
  Exemplo: "A segurança lógica física refere-se às medidas preventivas e reativas que protegem os recursos de hardware e software de uma organização."

- Aplicação na Empresa: Descrevam como estes conceitos foram entendidos e posteriormente implementados no ambiente da empresa. Isso pode envolver a instalação de sistemas de segurança físicos, a reestruturação da arquitetura de rede ou até mesmo a criação de protocolos internos.
  Exemplo: "Na empresa XYZ, implementamos sistemas de controle de acesso biométrico para garantir a segurança física de nossos servidores."

3.2.2 Detecção e Prevenção de Ataques

Conceitos de Segurança Lógica e Física e Valor da Informação:

- Segurança Lógica: Refere-se às medidas voltadas para proteger dados e informações digitais. Inclui controle de acesso, criptografia, políticas de senha, firewalls e detecção de intrusos, visando salvaguardar informações contra acessos não autorizados.

- Segurança Física: Trata da proteção dos recursos físicos de uma organização, como servidores, equipamentos de rede e centros de dados. Envolve a implementação de medidas como controle de acesso físico, câmeras de vigilância, alarmes e localização estratégica de equipamentos.

- Valor da Informação: Refere-se à importância dos dados e informações para uma organização. Reconhece-se que determinadas informações possuem maior valor, seja pelo seu conteúdo estratégico, confidencialidade ou impacto nos negócios.

Aplicação na Empresa:

Na CyberSecTips Ltda., a compreensão desses conceitos se manifestou de várias maneiras:

-Segurança Lógica: Foram implementadas políticas de controle de acesso rigorosas para restringir o acesso a informações confidenciais, utilizando autenticação multifatorial e criptografia de dados sensíveis armazenados nos servidores.

- Segurança Física: A empresa investiu na instalação de sistemas de controle de acesso físico, como leitores de cartões e câmeras de vigilância, para proteger fisicamente os servidores e o ambiente de armazenamento dos dados.

-Valor da Informação: Reconhecendo a importância dos dados, a empresa implementou protocolos internos para classificar e proteger informações sensíveis, garantindo que sejam manipuladas de acordo com as diretrizes de segurança estabelecidas.

Esses conceitos foram entendidos e aplicados de forma a proteger não apenas os dados digitais, mas também os recursos físicos da empresa, garantindo a integridade, confidencialidade e disponibilidade das informações.

4 CONCLUSÃO

Principais Descobertas e Propostas:

Durante o desenvolvimento do projeto de um chatbot de segurança da informação, identificamos a relevância da integração da Inteligência Artificial para aprimorar a eficácia na detecção e prevenção de ameaças cibernéticas. Implementamos técnicas de IA, como aprendizado de máquina, para melhorar a capacidade do chatbot em oferecer orientações de segurança personalizadas e proativas aos usuários.

Importância de Decisões Estratégicas Informadas em TI:

A tomada de decisões informadas em Tecnologia da Informação é fundamental para o sucesso de uma empresa. É crucial considerar não apenas os aspectos técnicos, como segurança e inovação tecnológica, mas também os administrativos, alinhando as estratégias de TI aos objetivos de negócios da empresa. Decisões bem embasadas em TI podem impulsionar a eficiência operacional, a competitividade no mercado e a adaptação às mudanças no ambiente empresarial.

Contribuições do Projeto para a Empresa Selecionada:

O projeto de implementação do chatbot de segurança da informação oferece contribuições significativas para a empresa CyberSecTips Ltda. Primeiramente, proporciona uma camada adicional de proteção para os usuários, orientando-os contra ameaças cibernéticas com dicas personalizadas e em tempo real. Isso promove a confiança dos clientes na empresa e reforça sua reputação como provedora confiável de soluções de segurança.

Além disso, a integração da IA no chatbot não apenas melhora a eficácia da segurança, mas também abre portas para futuras inovações. O aprendizado contínuo do chatbot pode ser utilizado para aprimorar outros serviços da empresa, como análise de dados para identificação de tendências de segurança, fornecendo insights valiosos para estratégias futuras.

Influência Positiva nos Objetivos e Operações Futuras:

Ao adotar e implementar estratégias de segurança da informação avançadas por meio da Inteligência Artificial, a empresa pode se posicionar à frente das ameaças cibernéticas emergentes.

Isso não apenas protege os ativos e dados críticos, mas também impulsiona a inovação contínua e a adaptabilidade a um cenário em constante mudança.

As melhorias na segurança e a capacidade de oferecer soluções personalizadas e proativas aos clientes podem aumentar a fidelidade e satisfação do cliente, impulsionando os objetivos de crescimento e expansão da empresa no mercado.