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

AI&SECTECH

SÃO JOÃO DA BOA VISTA, SP

OUTUBRO 2023

UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

AI&SECTECH

MÓDULO – INTELIGÊNCIA ARTIFICIAL

Inteligência Artificial – Prof. Rodrigo Marudi de Oliveira

Segurança em Sistema Computacionais - Prof. Nivaldo de Andrade

Estudantes:

Carolina Viana Bispo de Melo, RA 1012023100383
Eduardo Henrique Gonçalves, RA 1012023100212
Gabriel Cursino Alves, RA 1012023100197

SÃO JOÃO DA BOA VISTA, SP
OUTUBRO, 2023

SUMÁRIO

SUMÁRIO DE FIGURAS

1 INTRODUÇÃO

No panorama da segurança da informação, as pessoas e organizações enfrentam grandes desafios, sendo o phishing uma das ameaças pertinentes. Estatísticas alarmantes indicam que, em 2022, aproximadamente 80% de todos os ataques cibernéticos foram atribuídos a ataques de phishing. Este método representa uma preocupação significativa, especialmente para entidades empresariais, visto que pode roubar informações sensíveis, como senhas, números de cartão de crédito e dados de identificação pessoal.

Levando em consideração estes ataques, nosso projeto surge em resposta a este desafio, propondo uma abordagem para a integração de Inteligência Artificial e Segurança da Informação. O escopo central deste projeto é conceber uma estrutura que detecte e-mails que possivelmente são phishing.

A essência deste PI é desenvolver e implementar uma solução de IA que, além de otimizar os processos, garante a segurança e a confiabilidade com relação aos padrões de segurança vigentes. A proposta abraça a necessidade de proteger os sistemas contra vulnerabilidades potenciais.

O código apresentado, um detector de phishing baseado em processamento de linguagem natural e expressões regulares, serve como um exemplo prático dessa abordagem. Ao identificar padrões suspeitos e potenciais ameaças em conteúdos de e-mail, o sistema ilustra a capacidade da IA em contribuir ativamente para a prevenção de ataques cibernéticos, oferecendo um componente a mais para a segurança de sistemas computacionais.

Ao longo deste PI, será explorado a interseção entre IA e Segurança da Informação, destacando não apenas os desafios enfrentados, mas também as soluções propostas para fortalecer os indivíduos e as organizações em um cenário digital cada vez mais complexo.

2 DESCRIÇÃO DA EMPRESA

Tendo em vista as estatísticas de ataque de phishing no ano de 2022, nosso projeto não foi desenvolvido para uma empresa específica. Nosso objetivo foi ter uma iniciativa aberta e acessível a qualquer indivíduo, independentemente de pertencer a uma empresa ou a uma comunidade que esteja buscando reforçar suas defesas em relação aos roubos de informação. Diferentemente de uma abordagem voltada exclusivamente para uma empresa, nosso foco está na criação de uma solução universal, projetada para atender às necessidades de qualquer pessoa ou organização que busca aumentar sua segurança digital.

A proposta visa oferecer uma ferramenta prática e eficaz para a detecção de possíveis ameaças de phishing, uma das formas mais comuns de ataques cibernéticos. Ao integrar técnicas inteligência artificial e requisitos de segurança computacional, nosso objetivo é disponibilizar uma solução que vá além das barreiras corporativas, beneficiando qualquer usuário preocupado com a segurança de suas comunicações online.

3 PROJETO DE CONSULTORIA EMPRESARIAL

O foco deste PI abrange um contexto amplo e diversificado, não vinculado a uma empresa específica. Em um ambiente dinâmico e digital, nossa abordagem visa atender às necessidades de qualquer entidade, seja uma empresa local, uma startup, uma organização sem fins lucrativos ou um indivíduo.

Os desafios enfrentados incluem a necessidade de prevenção contra ameaças, proteger dados sensíveis e garantir a segurança das informações.

Portanto, esta não é uma resposta a desafios específicos de uma empresa, mas uma estratégia para enfrentar as ameaças em qualquer contexto. Esta abordagem visa oferecer uma ferramenta simples, que fortalecerá as defesas para uma operação digital mais segura.

3.1 INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial representa uma disciplina transformadora que está vinculada a diversos setores da sociedade contemporânea. Com ela, está a capacidade de desenvolver sistemas computacionais que podem realizar tarefas que normalmente exigiriam inteligência humana, tais como aprendizado, raciocínio, resolução de problemas e compreensão de linguagem natural.

A relevância da IA na atualidade ultrapassa as fronteiras acadêmicas, alcançando esferas práticas e estratégicas. A integração de IA não apenas automatiza processos, mas também oferece ideias a partir de volumes massivos de dados, impulsiona a eficiência operacional e impõe inovações substanciais. Seja na área da saúde, finanças, logística ou segurança da informação, a IA emerge como uma grande força para avanços significativos.

No contexto do projeto, a importância de integrar a IA é evidente. A integração de IA com Segurança em Sistemas Computacionais não só aprimora a eficácia operacional, mas também fortalece as defesas contra ameaças da internet. O aprendizado de máquina, uma vertente da IA, pode ser empregado para analisar padrões de comportamento, identificar anomalias e aprimorar a detecção de tentativas de phishing, como demonstrado no código desenvolvido.

3.1.1 INTRODUÇÃO À APLICAÇÃO DA IA

No contexto do Projeto Integrado, a aplicação prática da Inteligência Artificial é extremamente relevante, concentrando-se na detecção de ameaças, mais especificamente em

tentativas de phishing. Com o crescimento desses ataques, é necessário ter ferramentas para combater, e é aí que a IA surge como um aliado na prevenção e identificação dessas ameaças.

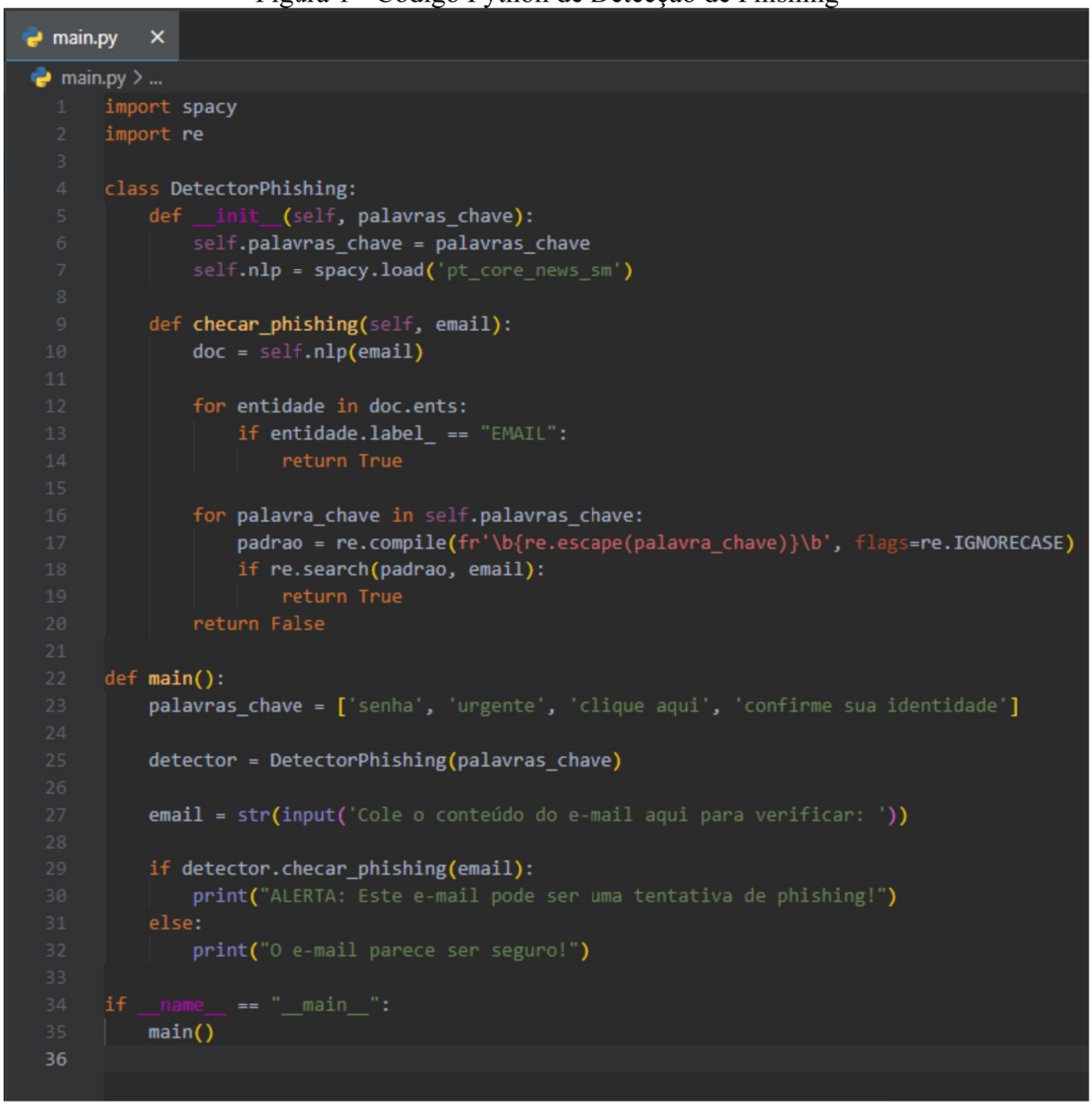
Um exemplo dessa aplicação está nos sistemas de segurança de grandes provedores de e-mail, como o Google com o Gmail. O Google utiliza IA e aprendizado de máquina para analisar padrões de comportamento de e-mails, identificar conteúdos suspeitos e classificar automaticamente mensagens potencialmente maliciosas na caixa de spam.

No PI em questão, a inspiração dessa aplicação prática se reflete no desenvolvimento do detector de phishing. O código apresentado utiliza a biblioteca Spacy para processamento de linguagem natural e expressões regulares para identificar padrões associados a tentativas de phishing. Essa abordagem não apenas exemplifica a aplicação de IA na detecção proativa de ameaças, mas também destaca como conceitos específicos, como processamento de linguagem natural, podem ser empregados para fortalecer as defesas cibernéticas.

Dessa forma, ao observarmos a aplicação de IA na detecção de phishing em e-mail, percebemos como a integração dessa tecnologia no projeto não apenas reflete práticas do mundo real, mas também oferece uma solução simples para a proteção de sistemas computacionais contra ameaças cibernéticas em constante evolução.

Abaixo segue uma imagem que proporcionará uma compreensão mais detalhada da estrutura e funcionalidades do detector de phishing, evidenciando a integração entre IA e Segurança em Sistemas Computacionais:

Figura 1 - Código Python de Detecção de Phishing



```python
import spacy
import re

class DetectorPhishing:
    def __init__(self, palavras_chave):
        self.palavras_chave = palavras_chave
        self.nlp = spacy.load('pt_core_news_sm')

    def checar_phishing(self, email):
        doc = self.nlp(email)

        for entidade in doc.ents:
            if entidade.label_ == "EMAIL":
                return True

        for palavra_chave in self.palavras_chave:
            padrao = re.compile(fr'\b{re.escape(palavra_chave)}\b', flags=re.IGNORECASE)
            if re.search(padrao, email):
                return True
        return False

def main():
    palavras_chave = ['senha', 'urgente', 'clique aqui', 'confirme sua identidade']

    detector = DetectorPhishing(palavras_chave)

    email = str(input('Cole o conteúdo do e-mail aqui para verificar: '))

    if detector.checar_phishing(email):
        print("ALERTA: Este e-mail pode ser uma tentativa de phishing!")
    else:
        print("O e-mail parece ser seguro!")

if __name__ == "__main__":
    main()
```

3.1.2 IMPLEMENTAÇÃO E TÉCNICAS UTILIZADAS

No desenvolvimento do projeto foram aplicadas técnicas de Inteligência Artificial para fortalecer a detecção de tentativas de phishing. Dentre as técnicas utilizadas, destaca-se o Processamento de Linguagem Natural (PLN).

O projeto incorpora o uso de PLN, onde a biblioteca Spacy é empregada para analisar e compreender o conteúdo dos e-mails. Através do PLN, o código busca identificar padrões específicos associados a tentativas de phishing, como termos sugestivos e estruturas linguísticas características dessas ameaças.

Além do PLN, expressões regulares são fundamentais na identificação de padrões específicos dentro do texto do e-mail. Essas expressões são construídas para capturar características associadas a mensagens de phishing, como solicitações de informações pessoais, links suspeitos e termos de urgência.

A implementação do código é realizada em Python, uma linguagem de programação amplamente utilizada em projetos de IA. Estruturas de dados como listas e expressões regulares são aproveitadas para manipular e analisar eficientemente o conteúdo dos e-mails. E a IA oferece um conjunto diversificado de técnicas, desde PLN até algoritmos de aprendizado de máquina, que podem ser aplicadas para aprimorar a eficácia da detecção.

Portanto, a Inteligência Artificial é a peça-chave que otimiza a capacidade de nosso projeto em enfrentar os desafios para construir uma defesa cibernética mais adaptável e protetiva.

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

A segurança em sistemas computacionais é um pilar essencial, que desempenha um papel crucial na proteção contra ameaças cibernéticas, como por exemplo, tentativas de phishing. A aplicação dos conceitos aprendidos nas aulas nos faz entender que este é um assunto que deve ser tratado com prioridade, e que devemos enfrentar os desafios associados à implementação desses princípios para garantir a proteção de dados.

A segurança compreende uma série de conceitos, desde a gestão de identidade e acesso até a implementação de protocolos de criptografia. No PI, a aplicação desses conceitos é evidente na proteção dos dados processados pelo detector de phishing. Além disso, garante a integridade e confidencialidade dos dados, refletindo os princípios fundamentais de segurança.

A implementação dos conceitos de segurança requer grandes desafios. O projeto deve se adaptar para lidar com as diversas formas e tentativas que o phishing podem assumir, e isso é um desafio constante. Com o aumento e avanço dos ataque de phishing, é exigido uma abordagem flexível, onde as atualizações e melhorias nos protocolos de segurança são essenciais para permanecer à frente das táticas dos adversários.

A importância da segurança computacional é para proteger a integridade dos dados e a confidencialidade das informações. A aplicação de conceitos de segurança fortalece a confiança dos usuários na utilização do detector de phishing.

3.2.1 CONCEITOS E IMPLEMENTAÇÃO DE SEGURANÇA

A segurança lógica refere-se às medidas preventivas que visam proteger os recursos de software e informações digitais de uma organização. Isso inclui a implementação de firewalls, antivírus e criptografia, garantindo a integridade, confidencialidade e disponibilidade dos dados. Já a segurança física diz respeito às medidas que protegem os ativos físicos de uma organização, como servidores, equipamentos de rede e instalações. Isso pode envolver o uso de câmeras de vigilância, sistemas de controle de acesso, sensores de movimento e outras medidas para evitar ou detectar intrusões físicas.

No PI a segurança lógica é incorporada nas técnicas de IA utilizadas para detectar ameaças de phishing. A aplicação de algoritmos de aprendizado de máquina, análise de padrões e processamento de linguagem natural representa uma camada de defesa lógica contra ataques cibernéticos. Embora o foco principal do projeto seja na segurança lógica, a segurança física também desempenha um papel indireto. A proteção dos servidores e

infraestrutura utilizada para implementar as soluções de IA contra acessos não autorizados é crucial. Embora não haja uma descrição detalhada das medidas específicas no código apresentado, as práticas recomendadas de segurança física são incorporadas na implementação global do projeto.

O valor da informação refere-se à importância e relevância dos dados para uma organização. Essa importância pode ser medida em termos de confidencialidade, integridade, disponibilidade e autenticidade das informações. O valor da informação guia a implementação de medidas de segurança, assegurando que os dados críticos sejam tratados com o devido cuidado.

No contexto do projeto, o valor da informação está diretamente ligado aos dados processados pelo detector de phishing. A confidencialidade desses dados é vital para garantir a confiança dos usuários e a eficácia do sistema. As técnicas de segurança lógicas implementadas buscam preservar o valor da informação ao proteger contra ameaças que visam comprometer a integridade e confidencialidade dos dados processados.

3.2.2 ARQUITETURA DE SISTEMAS

O objetivo do projeto é incorporar medidas protetivas para minimizar possíveis ameaças cibernéticas. Tendo isso em vista, não é um projeto desenvolvido para uma empresa específica, e sim uma solução que vá além das barreiras corporativas, beneficiando qualquer usuário preocupado com a segurança de seus dados.

Para antecipar e prevenir possíveis ameaças, implementamos algumas estratégias. Isso inclui a integração de técnicas IA para detecção de phishing, onde algoritmos de aprendizado de máquina são treinados para identificar padrões suspeitos nos e-mails processados.

Utilizamos como ferramenta, a linguagem Python que é amplamente utilizada em projetos de IA. Foi utilizada também a biblioteca Spacy para processamento de linguagem natural, que capacita o sistema a reconhecer padrões associados a tentativas de phishing. Além disso, a utilização de expressões regulares no código contribui para a identificação eficaz de termos e estruturas típicas de e-mails de phishing.

Essas ferramentas, integradas de maneira correta, formam uma abordagem abrangente que não apenas antecipa possíveis ameaças, mas também responde de maneira eficaz quando necessário. O uso de medidas protetivas contribui para a segurança no âmbito global.

4 CONCLUSÃO

Durante o desenvolvimento do projeto, aprendemos sobre integrar Inteligência Artificial e Segurança Computacional, proporcionando não apenas uma solução eficaz de detecção de phishing, mas também um aprendizado valioso sobre conceitos fundamentais nessas áreas.

Nossa iniciativa foi além dos limites de uma empresa específica, sendo projetada como uma ferramenta aplicável e acessível a qualquer indivíduo ou organização. O detector de phishing, fundamentado em processamento de linguagem natural, representa uma aplicação prática da IA na segurança da informação.

Com o aprendizado adquirido neste projeto, entendemos sobre a importância de integrar IA de maneira ética e segura, garantindo que as soluções desenvolvidas estejam alinhadas com padrões de segurança atuais. A integração entre IA e segurança é uma resposta às ameaças diárias.

Além dos benefícios da nossa solução de detecção de phishing, há os benefícios do aprendizado adquirido. Os conceitos de IA e segurança computacional, exploradas neste trimestre expandiram nosso conhecimento, capacitando-nos para enfrentar desafios no cenário digital.

Portanto, ao concluirmos o PI, não apenas criamos uma ferramenta para detecção de phishing, mas também saímos enriquecidos com o aprendizado necessário para construir um futuro digital mais seguro.