FIAP – Turma 2TDCPR [2024]
Disciplina: IA & Machine Learning
Checkpoint 1 - IA & Machine Learning
Professor: André Santos
Aluno: MATHEUS OLIVEIRA DA COSTA
RM: 552530

PARTE 1 - CONCEITOS

I. O PAPEL DA INTELIGENCIA ARTIFICIAL (IA) NA SEGURANÇA CIBERNETICA

Resumo: Presente na rotina na maioria das pessoas e principalmente nas organizações, a tecnologia tem sido a principal responsável para resoluções de problemas de forma inteligente, mas seu uso de forma inadequada pode abrir espaço para brechas nos sistemas da organização, ocasionando ataques mal-intencionados e vindo a causar prejuízos em larga escala. Com isso, esse trabalho tem o objetivo de apresentar o quanto a Inteligência Artificial é importante para as grandes, médias e pequenas organizações, auxiliando principalmente na identificação de ataques mal-intencionados e reforçando assim a segurança da informação (Zequim & Ribeiro, 2022).

O resumo no parágrafo anterior refe-se ao artigo “O papel da IA na Segurança Cibernética” de Zequim e Ribeiro, 2022. Os autores discorrem sobre o uso de sistemas inteligentes em benefício da segurança dos dados das empresas" e abordam a importância da IA na proteção de dados corporativos. O artigo explora como a IA pode ser utilizada por organizações de diferentes portes para identificar ataques mal-intencionados e reforçar a segurança da informação.

O estudo destaca que, embora a tecnologia tenha sido crucial para a resolução de problemas de forma inteligente, o uso inadequado de sistemas pode abrir brechas para ataques cibernéticos. O artigo também descreve os benefícios e desafios do uso de IA na segurança cibernética, como sua capacidade de aprender e responder automaticamente a ameaças. Além disso, discute tipos de ataques cibernéticos comuns, como Phishing e ZeroDay, e as ferramentas que utilizam IA para proteger dados.

O artigo conclui que o uso da IA na segurança cibernética está cada vez mais em demanda devido ao aumento de ataques cibernéticos, como ransomware, levando as empresas a investirem nessa tecnologia como medida proativa de proteção. Apesar de apresentar algumas desvantagens, como custos elevados e a necessidade de profissionais qualificados, os benefícios, como monitoramento contínuo, redução de erros humanos e otimização de processos, superam os desafios, tornando a IA essencial para a segurança da informação. A IA ainda requer tempo de adaptação, pois seu aprendizado é contínuo, mas é considerada vital para enfrentar ameaças em um ambiente digital cada vez mais complexo. Além disso, a adoção de IA é estratégica para a competitividade das empresas, protegendo dados e evitando prejuízos financeiros, enquanto também auxilia na conformidade com regulamentações de proteção de dados, como a LGPD, por meio do uso de tecnologias avançadas para análise e compreensão de documentos legais e corporativos.

Dadas as considerações gerais sobre o artigo mencionado, para responder às perguntas a seguir leia o respectivo artigo de Zequim & Ribeiro, 2023; seguindo estas instruções:

A. **Indique a página da resposta:** Especifique o número da página onde a resposta pode ser encontrada.
B. **Indique a seção e subseções:** Mencione a seção e quaisquer subseções relevantes onde a resposta está localizada.
C. **Teça comentários relacionando o artigo com tópicos discutidos em sala de aula:**
    a. Identifique a página do slide da aula corrobora com o seu argumento.
    b. Estabeleça uma conexão entre o conteúdo do artigo e os tópicos abordados em sala de aula.
    c. Ao responder às perguntas, certifique-se de fornecer informações precisas e relevantes.

Perguntas sobre o artigo de Zequim & Ribeiro, 2022:

1. Qual o principal objetivo da segurança cibernética? (ítens A, B e C)

Resposta: O principal objetivo da segurança cibernética é proteger a integridade, a confidencialidade e a disponibilidade de sistemas de informação, redes e dados contra acessos não autorizados, ataques cibernéticos e danos causados por agentes maliciosos ou falhas operacionais. Em suma, é um conjunto de boas práticas e ações para proteger um grupo de dados. (artigo, página 24 e 25, 4. Segurança Cibernética) (Em sala de aula, discutimos sobre confidencialidade, integridade e disponibilidade, no slide 12, esses pilares são apresentados como essenciais para mitigar riscos.)

2. O que é Phishing? (ítens A, B e C)

Resposta: Phishing é um ataque que, por meio de engenharia social, faz com que usuários entreguem seus dados e informações sigilosas. (artigo, página 26, 4.2 Tipos de ataques cibernéticos, subsecção: Phishing) (O tema do phishing foi revisitado durante a aula, quando discutimos técnicas de engenharia social, sendo enfatizado como uma das formas mais frequentes de ataques cibernéticos. No slide 15, foi apresentado um exemplo real de um e-mail de phishing.)

3. Como a inteligência artificial e a segurança cibernética trabalham juntas? (ítens A e C)

Resposta: A IA tem a capacidade de gerar e analisar dados automaticamente, incluindo banco de dados de logs extensos e conexões de rede, gerando inclusive uma resposta para os ataques, assim como um sistema imunológico. (Páginas: 26 e 27, seção: 5. Como a Inteligência Artificial e a Segurança Cibernética Trabalham Juntas) (Durante a aula, discutimos a função da IA na automação de processos de segurança, que está intimamente ligada à identificação de ameaças em tempo real. O slide 20 ilustra como a IA pode diminuir os tempos de resposta, um aspecto também destacado no artigo.)

4. Qual o marco histórico relacionado ao aumento de incidentes cibernéticos? (ítens A e C)

Resposta: Foi o aumento de ataques durante a pandemia de cerca de 394%, devido ao home office. (página: 27 e 28, seção: 6. Inteligência Artificial nas Empresas) (Esse crescimento foi abordado em nossas conversas sobre a fragilidade das redes domésticas e o efeito do

trabalho remoto na segurança da informação. No slide 25, analisamos os efeitos da pandemia no panorama da segurança digital.)

II. A UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA CIBERNÉTICA

A inteligência artificial (IA) está se tornando uma ferramenta cada vez mais valiosa na prevenção e detecção de ataques cibernéticos. Isso se deve à sua capacidade de processar e analisar enormes quantidades de dados de tráfego de rede, logs de sistema e outras fontes em tempo real. Além disso, os algoritmos de aprendizado de máquina (machine learning) permitem que a IA se adapte e melhore continuamente sua capacidade de detectar novas ameaças e táticas de ataque.

No entanto, é importante lembrar que a IA não é uma solução mágica para a segurança cibernética. Os cibercriminosos também estão usando IA para desenvolver ataques mais sofisticados. Portanto, é fundamental adotar uma abordagem de segurança em camadas que combine IA com outras ferramentas e práticas de segurança, além de investir em treinamento e conscientização dos usuários.

Assim, um dos grandes desafios que a área de segurança cibernética é **estruturar uma abordagem de segurança em camadas que utilize IA e outras técnicas e/ou práticas de segurança.** Essa abordagem multifacetada é crucial para garantir que, mesmo que uma camada seja comprometida, as demais continuem a oferecer proteção, resultando em uma defesa resiliente e adaptável contra ameaças cibernéticas.

5. Posto isso e com base nos conhecimentos adquiridos na disciplina de IA & Machine Learning, como você estruturaria uma abordagem de segurança em camadas, que utilize IA e outras técnicas e/ou práticas de segurança?

Resposta: A inteligência artificial pode ser utilizada em diversos quesitos, em firewalls e IPS, com algoritmos de Machine Learning para detectar logins ou conexões suspeitas,

monitoração e na análise de logs em tempo real.

PARTE 2 - APLICAÇÃO

- 1. Criar um repositório aberto da prova “disciplina_ia_c1_2024” (disponibilize o link de acesso).
- 2. Organizar o material do check-point 1 (prova, csvs, imagens) por pasta.
- 3. Desenvolver uma aplicação no Google Colab para responder/analisar os seguintes pontos:
    - Carregue a base de dados “urls_phishing_checkpoint1.csv” para o repositório no Github.
    - Gere uma amostra com 4000 observações (ver na tabela 1 qual semente utilizar).
    - Faça a EDA das URLs de phishing e legítimas para as variáveis “length_url”, “depth_url”, e “age_domain” (ver na tabela 1 qual variável deve utilizar).
    - Analisar no dataset (base de dados) “urls_phishing_checkpoint1_not_label.csv” quais domínios (coluna “domain”) tem maiores chances de conterem as urls de phishing?
    - De acordo com as suas análises qual a sua recomendação? Caso tenha identificado um possível ataque, qual deve ser a tomada de decisão para mitigar ou previnir o problema?
- 4. Carregar o Notebook no repositório “disciplina_ia_c1_2024”.
- 5. Finalizar o relatório executivo, salvar um PDF e carregar no diretório “disciplina_ia_c1_2024”.

Tabela 1. Parâmetros que devem ser utilizados por cada aluno para realizar a parte 2.

Alunos	“Semente” para amostra aleatória de 4000 observações	Variável para EDA
Demétrio de Freitas Oliveira	random_state = 42	length_url
Erik Alves da Silva	random_state = 7	length_url
Fabio Moraes do Amaral	random_state = 101	length_url
Gabriel de Oliveira Monteiro Batista	random_state = 2023	length_url
Gabriel Turcatti Conforto	random_state = 303	length_url

Higor Moura Santos	random_state = 17	depth_url
Ícaro Meirelles dos Santos	random_state = 85	depth_url
Mateus Rocha Pessoa	random_state = 123456	depth_url
Matheus Oliveira da Costa	random_state = 999	depth_url
Nícolas Miguel Bittencourt Tanajura	random_state = 2048	depth_url
Robert Leandro Lacerda	random_state = 31415	depth_url

Distribuição da pontuação da avaliação

Parte 1

1. Qual o principal objetivo da segurança cibernética? (1 pt)
2. O que é Phishing? (1 pt)
3. Como a inteligência artificial e a segurança cibernética trabalham juntas? (0,5 pt)
4. Qual o marco histórico relacionado ao aumento de incidentes cibernéticos? (0,5 pt)
5. Como você estruturaria uma abordagem de segurança em camadas com IA? (2 pts)

Parte 2

1. Criar repositório (0,25 pt)
2. O organizar repositório no GitHub (0,5 pt)
3. Desenvolver Notebook (2 pts)
4. Upload Notebook no GitHub (0,25 pt)
5. Relatório Executivo (2 pts)