INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO

Bruno Marques de Freitas
Caio Sérgio Xavier da Silva
João Vitor Valentim Pereira dos Santos
Maria Eduarda Alves Linhares
Pedro Henrique Teixeira Alves
Yasmin Felix Cordeiro

O TABULEIRO CIBERNÉTICO: EM QUE CASA ESTAMOS?

Cubatão
2023

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO

AUTORES

Bruno Marques de Freitas

Caio Sérgio Xavier da Silva

João Vitor Valentim Pereira dos Santos

Maria Eduarda Alves Linhares

Pedro Henrique Teixeira Alves

Yasmin Felix Cordeiro

O TABULEIRO CIBERNÉTICO: EM QUE CASA ESTAMOS?

Projeto apresentado ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – Campus Cubatão como parte dos requisitos necessários para a avaliação do componente Projeto Integrador do curso Técnico em Informática Integrado ao Ensino Médio, sob a orientação dos professores Maurício Neves Asenjo e Thiago Silva Augusto da Fonseca.

Cubatão

2023

RESUMO

O presente trabalho tem como intuito expor a guerra cibernética que ocorre entre os países Rússia e Ucrânia. Evidenciando ataques cibernéticos do conflito entre as nações, além de investidas que grupos de hackers usaram e usam para extrair informações e dados da população e como este fator interfere no âmbito da guerra, conjuntamente a importância da Inteligência Artificial - pode ser uma aliada na prevenção ou uma porta acesso a dados confidenciais - para estes ataques. A internet e redes sociais também influências seus usuários a seguirem uma determinada cultura ou modo de pensar, incluindo ideais políticos, por ser uma área de livre acesso. Métodos de prevenção e medidas a serem tomadas em caso de invasão são estabelecidas, a fim de ser um alerta sobre o crescente exponencial do crime de roubo de dados que vêm assolando o mundo, independentemente de estar ligado a conflitos geopolíticos. O trabalho foi elaborado para ser uma pesquisa bibliográfica.

Palavras-chave: Cibersegurança; ciberguerra; hacker(s); ataques; inteligência artificial.

ABSTRACT

The present work aims to expose the cyber warfare taking place between the countries of Russia and Ukraine. It highlights cyber attacks stemming from the conflict between these nations, in addition to the maneuvers that hacker groups have employed and continue to employ to extract information and data from the population. This factor's interference within the scope of warfare, coupled with the significance of Artificial Intelligence - which can serve as an ally in prevention or as a gateway to confidential data - for these attacks, is also emphasized. The internet and social networks also influence their users to adopt a certain culture or way of thinking, including political ideals, due to being a realm of unrestricted access. Methods of prevention and measures to be taken in case of intrusion are established to serve as a warning regarding the exponentially increasing crime of data theft that is plaguing the world, irrespective of its connection to geopolitical conflicts. The work was designed to be a bibliographic research.

Keywords: Cybersecurity; cyber warfare; hacker(s); attacks; artificial intelligence.

SUMÁRIO

INTRODUÇÃO

Nos últimos anos, a Rússia e a Ucrânia têm sido palco de uma série de conflitos políticos e militares. Um desses conflitos sendo inusitado até então, a ciberguerra. Nela, eles utilizam tecnologia para descobrir informações, comunicações e fazer sabotagens, obtendo uma vantagem significativa. Em 2022 por exemplo, um grupo ligado a inteligência militar russa implementou um Industroyer – malware[1] –, contra as subestações de alta tensão na Ucrânia, em coordenação com a invasão russa (REVISTA VEJA, 2022).

Por consequência, governos estão criando grandes planos em âmbito virtual para sair na dianteira de guerras, organizando equipes para prevenir possíveis ataques na rede e até mesmo integrando hackers ao seu exército.

Para compreender este Projeto Integrador, primeiro será necessário entender alguns termos básicos que são essenciais no desenvolver do tema abordado. Dado e Informação, aparentam possuir o mesmo significado, porém são termos distintos.

Dado

Quando pesquisamos no Google a palavra "dado", é exibida a seguinte definição: “1. Que se deu; concedido, oferecido. 2. Que se conhece, que se sabe por antecipação.”. Por estas definições, temos a palavra dado sendo compreendida como conhecimento. O artigo escrito por Valdemar W. Setzer, pelo departamento de Ciências da Computação da Universidade de São Paulo, define dado como um conjunto de símbolos quantificados ou quantificáveis. Uniremos os dois significados para chegar à uma definição mais precisa. Dado é, portanto, um conjunto de símbolos que se conhece, como as letras de um alfabeto, imagens ou sons.

Com esta definição, um dado é necessariamente uma entidade sintática, ele não possui um significado direto, sendo apenas a representação de algo. Um computador por exemplo, recebe um dado, trabalha este dado de maneira interna e realiza a exibição dele, seja ele uma imagem, um texto ou som. Além de conseguir interpretar e manipular o dado, o computador também possui a capacidade de armazená-lo.

Por ser algo de valor quantificado a manipulação do dado feita pelo computador, se restringe a estas duas ações: manipular e armazenar. Exemplos: em textos, consegue-se mudar a formatação, tamanho da fonte e até mesmo a estética das palavras empregadas. Em imagens, a alteração das cores, formatação, recorte e as habilidades de edição.

Dado, é um conjunto de símbolos que usamos para representar algo, mas que sozinho não possui significado. Então, como pode virar algo tão valioso e que deve ser protegido com alto nível de segurança? A resposta é mais simples do que parece, para compreender um dado precisa-se ter conhecimento e entender o que aquele símbolo está representando. A habilidade de compreender um trato, transforma-o em informação tornando-a algo precioso.

Informação

A informação é uma abstração informal, que se encontra na mente de uma pessoa e possui importância/significado para ela. Para que haja o entendimento da informação, é necessário que além da importância, o indivíduo possua conhecimento sobre do que se trata a informação e seus componentes. Na frase “Veneza é bela”, para compreensão correta, o ouvinte terá de possuir o conhecimento de que Veneza é uma cidade e não um país, e para concordar com a afirmação, necessita também que o ouvinte conheça a estrutura da cidade. Caso não tenha o conhecimento destas duas coisas, a frase não fará sentido e será apenas um dado irrelevante. Deste modo, não é possível processar informação diretamente em um computador. Para isso é necessário reduzi-la a dados.

Se esta informação fosse armazenada em um computador, sua entrada seria um dado, pois a máquina não consegue compreender o que está sendo representado. Uma vez armazenada, ela poderá sofrer alterações de forma estrutural, mudança na cor de suas letras ou até ter a palavra “Veneza” trocada por “Santos” que o computador não perceberia a alteração no sentido da frase, pois manipulou o dado de forma sintática, diferente do receptor, que irá perceber a alteração de forma semântica. Deste modo, não é possível processar informação diretamente em um computador. Para isso é necessário reduzi-la a dados.

Aplicação

Ao passar dos anos os avanços tecnológicos, possibilitaram que cada vez mais os dados fossem armazenados em máquinas como computadores e celulares. O que garantia uma segurança para as pessoas que utilizam deste método, pois diminui-se drasticamente o risco de perda. Documentos, fotos e áudios, passaram a ter uma maior circulação dentro das máquinas. Graças à internet, estes dados também fluem fora dela, passando de uma máquina para outra, através das ondas eletromagnéticas que estão presente em todo globo terrestre, possibilitando uma interação global entre máquinas e pessoas.

Como foi dito anteriormente, a informação é um dado com relevância, que quando armazenada em uma máquina se transforma em dado, até ser exibida a um receptor que a compreenderá de forma semântica, tornando-se novamente uma informação. Ao armazenar uma foto em nosso celular e enviá-la para alguém, estamos realizando uma transferência de dados, que ao ser exibida para quem enviamos, lhe informará algo, caso ela tenha conhecimento do que se trata a imagem.

Até esta imagem chegar à pessoa desejada, ela percorre milhares de quilômetros em segundos, este percurso na grande maioria das vezes é seguro, porém, no meio dele, alguma pessoa má intencionada pode interceptar o dado e manipulá-lo. E até mesmo a pessoa a qual o dado foi destinado, pode agir de má fé e exibi-lo sem sua permissão. Esta interceptação ou exibição sem consentimento pode lhe gerar sérios problemas.

Unidades Governamentais não estão livres destas situações, por isto, além das criptografias, um número cada vez menor de pessoas possuem acesso a determinadas informações, quanto mais importante menos pessoas têm acesso, como o investimento em setores, planos de guerras, projetos em desenvolvimento e documentos. A exposição ou extração (caso seja hackeado) destas informações, podem deixar um país vulnerável a ataques de países rivais (se houver conflitos pré-estabelecidos), que sua economia e segurança caia, tendo por consequência, desordem e preocupação da população, que pode acarretar um maior caos interno.

Ao decorrer deste trabalho, abordaremos como a exposição de dados e acesso a informações confidenciais de um país, são utilizados contra ele, causando guerras e aumentando o conflito já existente. A guerra entre a Rússia e a Ucrânia é um conflito em que diversos ataques foram possibilitados graças a interceptação de informações.

OBJETIVOS

Objetivo Geral

Apresentar e explicar a Guerra Cibernética que ocorre entre a Rússia e a Ucrânia.

Objetivos Específicos

Relatar o contexto histórico em que esta guerra se iniciou. Abordar temas, sociais, políticos, econômicos, culturais e o relacionamento entre os dois países europeus. Apontar características e consequências da guerra e crimes cibernéticos que ocorreram, que são conhecidos por agravar cada vez mais este conflito. Analisar a estrutura de um ataque cibernético.

MATERIAIS E MÉTODOS

Foi realizada uma revisão bibliográfica a fim de obter informações relevantes e atualizadas que contribuam para a compreensão e aprofundamento do assunto. Para isso, foram consultados artigos científicos disponíveis online e impressos, livros especializados, teses, dissertações e outros materiais pertinentes. Essa revisão permitiu uma análise comparativa das diferentes fontes, a fim de compreender as crises externas e internas relacionadas a esse conflito, assim como suas consequências no mundo virtual e físico, tanto em território nacional quanto estrangeiro.

As fontes consultadas proporcionaram uma visão ampla e aprofundada sobre o tema, permitindo o mapeamento das diferentes perspectivas e análises existentes. A partir dessas informações, será possível estabelecer um diálogo crítico e embasado, analisando tanto as repercussões dentro dos territórios nacionais envolvidos, quanto em âmbito internacional.

1 CIBERGUERRA: RÚSSIA X UCRÂNIA

Ciberguerra é um termo usado para descrever conflitos no ciberespaço que envolvem ataques e contra-ataques contra sistemas de computadores e redes de comunicação. É um tipo de guerra travada principalmente através de ataques cibernéticos, como invasão de sistemas, roubo de dados, interrupção de serviços e disseminação de malware.

Ao contrário da guerra tradicional, a guerra cibernética não envolve necessariamente ações físicas diretas ou o uso de armas convencionais. Em vez disso, o ataque é realizado por meio de computadores, redes e outros dispositivos conectados à Internet. Governos, organizações criminosas ou grupos de hackers patrocinados pelo estado podem estar envolvidos. Os objetivos da guerra cibernética podem ser distintos das costumeiras guerras. Alguns países podem buscar vantagem militar, espionagem ou roubo de propriedade intelectual. Outros podem tentar interromper a infraestrutura crítica, como energia, transporte ou sistemas de comunicação, com o objetivo de causar instabilidade ou perda econômica.

Os ataques cibernéticos podem ser realizados de variadas formas, como phishing, negação de serviço (DDoS), exploração de vulnerabilidades no sistema, espionagem cibernética e sabotagem de infraestruturas digitais. À medida que a tecnologia avança, também avançam os métodos e o poderio dos ataques cibernéticos, tornando a guerra cibernética uma preocupação crescente para governos, empresas e indivíduos em todo o mundo.

1.1 Quais são as implicações geopolíticas da ciberguerra entre Rússia e Ucrânia para a segurança regional e global e quais são as possíveis soluções para esse conflito?

A principal implicação geopolítica presente na Guerra Rússia x Ucrânia, está presente na relação que se deu início a guerra, o ingresso da Ucrânia na OTAN e o sentimento russo como um ataque a sua integridade.

Outros conflitos anteriores também influenciaram para concretização desse conflito como sentimento russo de repatriar países separatistas após a dissolução da URSS e a invasão da Rússia á Crimeia em 2014.

Com isso, há e haverá efeitos da guerra em diversas áreas. Como na sociedade, em que mais de 8 milhões de ucranianos buscaram refúgio em outras nações da Europa, enquanto aproximadamente 6 milhões procuram por lugares para se abrigar dentro da Ucrânia graças a destruição causada pela guerra.

Já na política, a instabilidade e a tensão política são efeitos da guerra muito delicados nas relações internacionais que podem gerar mais conflitos ou sanções econômicas que geram crises, tal qual a Rússia, que cortou o fornecimento de Gás Natural para a Europa, e assim gerando uma crise energética durante o inverno europeu onde a energia e aquecimento aumentaram drasticamente. A economia também foi afetada pelo não funcionamento de usinas nucleares na região de Donbass no Leste e Sul da Ucrânia, região essa de interesse russo por ser economicamente ativa e estratégica economicamente.

As soluções para os efeitos da guerra citados anteriormente só virão a partir de uma mobilização global e de negociações diplomáticas principalmente de países da OTAN para a reconstrução do país semelhante ao que aconteceu com o Japão pós-Segunda Guerra Mundial junto com a flexibilização de acordos do lado dos russos e da OTAN.

1.2 Qual é o papel dos ataques cibernéticos na estratégia militar da Rússia e da Ucrânia e como esses ataques se integram às operações militares convencionais?

A guerra é uma junção de diversos ataques a um determinado território, seja um país, cidade, ou um conjunto deles. Estes ataques são extremamente bem elaborados para que seu resultado saia como o país atacante planejou. Com a internet e a tecnologia, não se é mais necessário a locomoção de batalhões ou tropas militares para isto. Dê uma sala com computadores, é possível atacar um país inteiro e desestruturar sua rede de segurança.

Ataques como o Distributed Denial of Service ou, em inglês, ataque distribuído de negação de serviço (DDoS), geralmente utilizados para derrubar sites importantes, como os de bancos. E o NotPetya de 2017, a Ucrânia teve a companhia nacional de energia e o principal aeroporto do país afetados, além de diversos outros distúrbios, ataque causado pelo setor de

inteligência do governo russo. São os mais danosos e eficientes, pois atingem diretamente a população, desequilibrando o andamento social e exigindo cada vez mais segurança para o governo.

Luca Belli, professor da FGV Direito Rio e coordenador do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas (FGV) afirmou, "80% da Ucrânia ficou paralisada por causa do NotPetya. Para dar um exemplo concreto: o sistema de monitoramento de radiação em Chernobyl ficou desativado por várias horas. Imagine o componente psicológico desse tipo de ataque, que deixa o alvo completamente perdido".

Os ataques cibernéticos em sua grande maioria de ações, possui a finalidade de desestruturar o governo, seja de forma indireta, ataques que atingem a população, mas não ao sistema governamental, ou direta, ataques diretamente aos sistemas do governo. Um tipo de ataque comum na guerra entre a Rússia e a Ucrânia é o data wiper (apagador de dados), destaca Belli, “é um software malicioso que infecta e apaga bancos de dados”.

Invadir um local com força bruta após ser atingido por ciberataques demanda menos estratégia em campo e armamento, pois o ambiente que sofrerá o ataque, não se encontra com forças bélicas suficientes para defender-se, em razão de estar se recuperando do ataque cibernético sofrido anteriormente.

Além de priorizar seus soldados pelo menor número de conflitos físicos, os ataques cibernéticos não ocorrem somente por meio de hackers. Ao apertar de um botão, bombas e mísseis são lançados por um computador com toda a sua trajetória já estabelecida. O lançamento só necessita da intervenção humana para colocar as coordenadas do local de queda e para a liberação do lançamento.

A guerra entre a Rússia e a Ucrânia é conhecida por ser uma guerra hibrida, onde os conflitos cibernéticos são tão importantes como os físicos. A Rússia por possuir maior tecnologia e preparo para isso, se destaca e têm ganho os principais conflitos, conseguindo cada vez mais dados e desestabilizando ainda mais a Ucrânia, dificultando a formação de estratégias do país, para se reerguer na tentativa de mudar o cenário atual deste conflito.

1.3 Como as operações de ciberguerra entre Rússia e Ucrânia afetam a segurança e a privacidade dos usuários de internet em ambos os países e como as agências governamentais estão lidando com esse problema?

As operações da ciberguerra referem-se a um conjunto de atividades cibernéticas que visam comprometer a integridade, confidencialidade ou disponibilidade de sistemas de informação, infraestruturas críticas e dados. Essas atividades podem ser realizadas por governos, organizações criminosas, ativistas políticos e outras entidades com motivações diversas. As operações da ciberguerra podem incluir ataques cibernéticos, roubo de dados. A ciberguerra pode afetar diretamente a segurança dos usuários online. Através de ataques cibernéticos, hackers podem acessar informações pessoais, senhas, contas bancárias e outras informações confidenciais de utilizadores. Além disso, esses ataques podem afetar a infraestrutura de sistemas de comunicação e serviços essenciais, como energia, água, saúde e transportes, causando prejuízos financeiros e interrupções nos serviços públicos.

A ciberguerra é uma realidade crescente no mundo contemporâneo, e as operações cibernéticas são um componente crucial desses conflitos. A ciberguerra envolve ações hostis realizadas por governos, organizações criminosas e ativistas políticos em ambientes virtuais. Infelizmente, os usuários online em países vítimas da ciberguerra são afetados de várias maneiras. Esses ataques podem ter um efeito cascata em toda a economia do país, causando danos significativos e comprometendo a segurança nacional. Esses ataques são frequentemente realizados por governos estrangeiros que visam comprometer sistemas de defesa e infraestrutura crítica. Além disso, os usuários online em países vítimas da ciberguerra também podem ser alvos de espionagem cibernética. Isso pode incluir a coleta de informações pessoais e financeiras, como senhas e dados bancários, bem como informações sensíveis relacionadas à política e à segurança nacional. Essas informações podem ser usadas para fins de extorsão ou chantagear indivíduos ou organizações para obter vantagens políticas ou financeiras.

Os usuários online em países vítimas da ciberguerra também estão vulneráveis a diversos tipos de ataques cibernéticos, como phishing, malware, negação de serviço, ransomware e outros tipos de ataques. Esses ataques são geralmente realizados com o objetivo

de causar danos, roubar informações confidenciais ou obter acesso não autorizado a sistemas e redes, roubar informações confidenciais e infectar dispositivos com malware. Os criminosos cibernéticos usam técnicas de engenharia social para enganar os usuários a clicar em links maliciosos ou abrir anexos de e-mails que contêm malware. Isso pode levar à perda de informações pessoais e governamentais, como estratégias de guerra, segredos comerciais ou segredos de Estado. Em resposta às operações da ciberguerra, muitos governos e organizações implementaram medidas de segurança cibernética para proteger seus sistemas e dados. Isso inclui a implementação de firewalls, criptografia de dados, testes de penetração e monitoramento de rede.

Em resumo, as operações da ciberguerra representam uma ameaça significativa à segurança cibernética global. É crucial que indivíduos e organizações tomem medidas de segurança adequadas para proteger seus sistemas e dados contra esses ataques. A colaboração internacional também é fundamental para identificar e neutralizar ameaças cibernéticas em todo o mundo.

1.4 Quais são as principais vulnerabilidades, táticas, estratégias e ameaças enfrentadas pelos sistemas de informação e infraestrutura crítica da Ucrânia e como a Rússia tem explorado essas vulnerabilidades?

Ao longo desses anos de intenso conflito entre Rússia e Ucrânia, já houveram diversos ataques, desde a anexação da Crimeia em 2014 (BRITISH BROADCASTING CORPORATION, 2014), até o ataque de mísseis em território ucraniano em 2022 (GLOBO COMUNICACAO E PARTICIPACOES S/A, 2022). Ainda a alguns anos, em 2015 e 2017, um ataque cibernético interrompeu totalmente o fornecimento de energia elétrica na Ucrânia (ROHR, 2017).

No primeiro movimento, o país atacante, faz uma investida a infraestrutura crítica – como nos ataques citados acima em 2015 e 2017. Eles buscam interromper os serviços essenciais, água, energia elétrica e transporte. Esse ataque tem como objetivo causar danos imensos, afetar a economia e a segurança nacional. Outros movimentos temos:

a) **ataque DDoS**: os ataques DDoS visam sobrecarregar um servidor com tráfego excessivo, tornando-o inacessível. O objetivo é interromper a operação do servidor ou do serviço afetado. Na guerra entre a Rússia e a Ucrânia, os ataques DDoS foram usados para interromper sites do governo e outros serviços online;
b) **injeção de malware**: a injeção de malware tem como objetivo infectar um sistema ou rede com um software malicioso. Esse tipo de ataque pode ser usado para obter acesso não autorizado a sistemas, coletar informações confidenciais ou controlar sistemas remotamente. Na guerra cibernética entre Rússia e Ucrânia, o malware foi usado para monitorar a atividade de usuários de computador, coletar informações e controlar sistemas;
c) **ataques de negação de serviço a sistemas de infraestrutura crítica**: os ataques de negação de serviço a sistemas de infraestrutura crítica visam interromper serviços essenciais, como energia elétrica, água e transporte. Esses ataques têm como objetivo causar danos significativos e afetar a economia e a segurança nacional do país afetado;
d) **ataques a sistemas de votação**: os ataques a sistemas de votação têm como objetivo manipular os resultados de eleições ou minar a confiança pública no processo eleitoral. Na guerra entre Rússia e Ucrânia, os ataques a sistemas de votação foram usados para comprometer as eleições e influenciar o resultado das eleições;
e) **ataques a empresas e instituições financeiras**: os ataques a empresas e instituições financeiras têm como objetivo causar danos financeiros significativos. Esses ataques podem envolver roubo de informações confidenciais, interrupção dos serviços online e transferência de dinheiro para contas controladas pelos hackers. Na guerra entre Rússia e Ucrânia, os ataques a empresas e instituições financeiras foram usados para causar interrupções e danos econômicos;

f) **ataques de phishing**: os ataques de phishing são usados para obter acesso não autorizado a contas de e-mail e outras informações confidenciais. Os hackers enviam e-mails falsos com links maliciosos ou anexos que, quando clicados, instalam malware no computador da vítima. Esses ataques foram usados para obter informações confidenciais de funcionários do governo e outras pessoas de interesse;

g) **uso de bots e trolls**: os bots e trolls são usados para disseminar desinformação e propaganda online. Os bots são programas de computador que podem ser programados para amplificar mensagens específicas ou espalhar notícias falsas. Os trolls são pessoas reais que são pagas para espalhar desinformação e propaganda. O objetivo é influenciar a opinião pública e criar divisões dentro do país afetado. Na guerra entre a Rússia e a Ucrânia, os bots e trolls foram usados para espalhar propaganda e criar divisões.

2 AFINAL QUEM SÃO OS REIS E RAINHAS DA INTERNET

2.1 Como as plataformas de redes sociais estão moldando a cultura e a política na era digital e quem são os influenciadores mais poderosos nessas plataformas?

As redes sociais têm se tornado espaços vitais para a interação social e política. Por meio dessas plataformas, os usuários compartilham informações, participam de debates, expressam opiniões e se mobilizam para causas sociais e políticas. A facilidade de acesso e alcance global das redes sociais torna-as um ambiente propício para a difusão de ideias e valores culturais.

Elas moldam a opinião pública e a mobilização política. A disseminação rápida de informações, muitas vezes impulsionada por algoritmos de recomendação, pode criar bolhas de opiniões, onde os usuários são expostos principalmente a conteúdos que reforçam suas crenças preexistentes (BAKSHY et al., 2015). Isso pode influenciar a percepção da realidade e polarizar debates políticos.

E dentro desse cenário, deu-se origem a uma nova geração de influenciadores, pessoas que conquistaram muitos seguidores e exercem influência sobre suas opiniões e comportamentos. Pessoas como Elon Musk, com sua presença marcante no Twitter, têm o poder de mover mercados financeiros e moldar a narrativa sobre inovação tecnológica (CHAVKOWSKI, 2021). A influência das redes sociais na cultura e política pode ter consequências significativas. A polarização política, a disseminação de informações falsas e o risco de manipulação de opiniões são desafios importantes associados ao uso dessas plataformas (VOSOUGHI et al., 2018).

Aqui demonstra mais um exemplo de como a concentração de poder pode limitar a diversidade de vozes e de perspectivas.

Para minimizar os impactos negativos do uso das redes sociais na cultura e política, é necessário a ciberliteratura e transparência nas políticas de moderação no conteúdo de plataformas. Além disso, regulamentações que abordem a disseminação de desinformação e a privacidade dos usuários.

2.2 Como a privacidade e a segurança dos usuários da internet é afetada com a concentração de poder nas mãos de um pequeno calibre de pessoas ou entidades?

A partir da crescente dependência das tecnologias digitais houve também preocupações a respeito da privacidade de informações pessoais e segurança das comunicações online (SMITH et al., 2020).

Existe um pequeno número de empresas de tecnologia que exercem influência desproporcional sobre a infraestrutura digital e os serviços online que evidenciam a concentração de poder na internet. Entre elas, as “Big Techs” como Google, Facebook (agora Meta), Amazon e Apple têm desempenhado um papel dominante (MOROZOV, 2019). Empresas como essas, controlam plataformas essenciais para a comunicação, pesquisa e entretenimento, com isso possuem a capacidade de influenciar diretrizes, padrões e políticas relacionadas à privacidade e segurança.

A coleta massiva de dados pessoais por essas empresas para fins de publicidade direcionada e personalização de conteúdo levanta preocupações quanto ao controle sobre as informações compartilhadas (TUROW et al., 2018). A centralização do acesso a dados cria um desequilíbrio entre usuários e entidades, o que resulta em uma perda de controle sobre o uso de suas informações e isso amplia as vulnerabilidades de segurança online.

Um caso notório é o vazamento de dados da Equifax em 2017, uma das três principais agências de crédito nos Estados Unidos. O ataque cibernético resultou no roubo de informações pessoais sensíveis de 147 milhões de consumidores (FINKLE; RUCINSKI, 2019). Essa vulnerabilidade foi agravada pela centralização de poder nas agências de crédito, onde uma única entidade continha informações críticas de muitos indivíduos.

Com empresas dominantes como no caso do parágrafo anterior, nos leva a ter pouca diversidade online já que elas podem impor suas próprias visões e limitar a exposição a perspectivas diversas. Um exemplo é a disseminação de Oormação e notícias falsas em redes

sociais de grande porte, que podem afetar negativamente a diversidade de opiniões e a qualidade do debate público (GUESS et al., 2019).

Além de empresas, países exercem esse mesmo papel como a Rússia que tem sido ativa na promoção de suas agendas políticas e interesses por meio do uso estratégico das tecnologias digitais (RID, 2019).

A Rússia ganhou notoriedade por suas campanhas de desinformação e propaganda nas redes sociais e outras plataformas digitais. Casos como a interferência nas eleições presidenciais dos Estados Unidos em 2016 e as tentativas de influenciar outras eleições em todo o mundo evidenciam como os atores russos aproveitam as vulnerabilidades da concentração de poder para disseminar informações enganosas e promover agendas políticas específicas (HOWARD; KOLLANVI, 2016).

Além de suas atividades de desinformação e ciberataques, a Rússia também implementou medidas de regulação e censura digital para exercer controle sobre a narrativa online. Leis como a “Lei de Soberania da Internet” permitem que o governo russo restrinja o acesso a informações e controle o tráfego da internet, ampliando sua influência sobre o espaço digital (ISACHENKOV, 2019).

3 HACKERS: OS CAÇADORES VIRTUAIS.

3.1 Hackers e sua identificação

O cenário digital contemporâneo tem sido marcado pela crescente incidência de invasões de redes e violações de segurança cibernética. A figura do hacker muitas vezes é associada a atividades maliciosas, porém, a compreensão completa dos hackers e de suas motivações é essencial para lidar com os desafios da segurança cibernética de forma eficaz.

Hackers são indivíduos altamente habilidosos em informática, capazes de explorar vulnerabilidades em sistemas e redes de computadores. Eles não constituem um grupo homogêneo, mas sim uma comunidade diversificada com diferentes motivações e objetivos. Hackers podem ser classificados em categorias distintas. Sendo elas:

a) **hackers éticos (White Hats)**: são especialistas em segurança cibernética que utilizam suas habilidades para identificar e corrigir vulnerabilidades, visando fortalecer a proteção de sistemas e redes;
b) **hackers maliciosos (Black Hats)**: são hackers que buscam explorar vulnerabilidades para obter ganhos pessoais ou prejudicar indivíduos, organizações ou governos;
c) **hackers grey hats**: eles operam em uma zona intermediária entre as categorias ética e maliciosa, muitas vezes revelando vulnerabilidades sem permissão, mas com intenções questionáveis.

3.1.1 Motivações de hackers para invasões de redes

As motivações que levam hackers a invadir redes podem variar significativamente e podem incluir:

a) **ganho financeiro**: alguns hackers buscam obter lucro financeiro através de atividades como extorsão, fraude, roubo de informações pessoais ou bancárias;

b) **espionagem cibernética**: hackers envolvidos em espionagem cibernética buscam coletar informações sensíveis de organizações ou governos para benefício próprio ou para vender a terceiros;
c) **ativismo e causas ideológicas**: hackers ativistas, também conhecidos como hacktivistas, invadem redes para expressar pontos de vista políticos, sociais ou ideológicos e causar impacto em instituições ou governos;
d) **desafio técnico**: algumas invasões de redes são motivadas pelo desejo de superar desafios técnicos, demonstrando suas habilidades ou ganhando reconhecimento entre a comunidade hacker.

3.1.2 Atividades de hackers em invasões de redes

As atividades realizadas por hackers durante invasões de redes podem variar desde a exploração de vulnerabilidades até a extração de dados sensíveis. Algumas das atividades mais comuns são:

a) **exploração de vulnerabilidades**: hackers identificam e exploram vulnerabilidades em sistemas e redes para obter acesso não autorizado;
b) **roubo de dados**: hackers podem roubar informações sensíveis, como dados pessoais, financeiros ou industriais, para uso próprio ou para venda;
c) **ataques de negação de serviço (DDoS)**: hackers podem usar uma rede de dispositivos comprometidos para inundar um sistema com tráfego, tornando-o inacessível;
d) **injeção de código malicioso**: hackers inserem código malicioso em sites ou aplicativos para obter acesso a informações ou controlar sistemas.

A categorização dos hackers em diferentes tipos e a análise de suas motivações oferecem insights valiosos para a proteção de sistemas e redes contra ameaças cibernéticas.

3.2 Quais são as principais técnicas e ferramentas usadas pelos hackers para explorar vulnerabilidades em sistemas e redes de computadores?

Os hackers utilizam uma variedade de técnicas e ferramentas para explorar vulnerabilidades em sistemas e redes de computadores. Essas técnicas podem ser usadas para encontrar brechas de segurança e ganhar acesso não autorizado a sistemas. Aqui estão algumas das principais técnicas e ferramentas que os hackers podem usar:

a) **varredura de portas (Port Scanning)**: os hackers usam ferramentas de varredura de portas para identificar quais portas de rede estão abertas em um sistema. Portas abertas podem indicar serviços ou aplicativos em execução, que podem ser alvos para ataques;
b) **enumeração**: a enumeração envolve a coleta de informações sobre sistemas e redes, como nomes de usuários, grupos, serviços e recursos compartilhados. Isso ajuda os hackers a entenderem a estrutura da rede e identificar alvos potenciais;
c) **exploração de vulnerabilidades**: os hackers procuram por vulnerabilidades conhecidas em sistemas e aplicativos. Eles usam ferramentas automatizadas, como scanners de vulnerabilidades, para encontrar falhas de segurança que podem ser exploradas para obter acesso não autorizado;
d) **ataques de força bruta e dicionário**: os hackers usam ferramentas para tentar adivinhar senhas ou chaves criptográficas, tentando uma ampla gama de combinações até encontrar a correta. Isso é conhecido como ataque de força bruta ou ataques de dicionário;
e) **ataques de injeção**: isso inclui ataques como SQL Injection e Cross-Site Scripting (XSS), onde os hackers inserem código malicioso em campos de entrada para explorar falhas em aplicativos da web e obter acesso a dados ou executar comandos não autorizados;
f) **man-in-the-middle (MitM)**: nesse tipo de ataque, um hacker intercepta a comunicação entre dois pontos, podendo capturar informações confidenciais, como senhas, sem o conhecimento das partes envolvidas;

g) **ataques de negação de serviço (DoS/DDoS)**: hackers podem inundar um sistema ou rede com tráfego excessivo, causando a indisponibilidade dos serviços. No caso de ataques distribuídos (DDoS), várias máquinas são coordenadas para aumentar a intensidade do ataque;
h) **malware**: hackers criam e distribuem malware, como vírus, worms, trojans e ransomware, que podem se infiltrar em sistemas e redes para realizar atividades maliciosas, como roubo de informações ou controle remoto;
i) **engenharia reversa**: os hackers podem desmontar e analisar aplicativos ou software para encontrar vulnerabilidades ou extrair informações confidenciais;
j) **engenharia social**: como mencionado anteriormente, os hackers também usam a engenharia social para obter informações dos usuários, explorando suas fraquezas psicológicas.

3.3 Como as empresas e organizações podem proteger seus sistemas e dados contra-ataques de hackers, incluindo o uso de firewalls, sistemas de detecção de intrusos e políticas de segurança?

Ao adotar uma abordagem abrangente de segurança cibernética, as empresas e organizações podem fortalecer suas defesas contra ameaças cibernéticas e proteger seus sistemas e dados de forma mais eficaz através do uso de firewalls e sistemas de detecção de intrusos e políticas de segurança. Alguns exemplos da funcionalidade de cada ferramenta são:

a) **firewalls**: utilizar firewalls para monitorar e controlar o tráfego de rede, permitindo apenas o acesso autorizado e bloqueando tentativas de invasão;
b) **sistemas de detecção de intrusos (IDS) e sistemas de prevenção de intrusos (IPS)**: essas ferramentas ajudam a identificar atividades suspeitas na rede e podem bloquear automaticamente tentativas de ataques;
c) **políticas de segurança**: desenvolver e implementar políticas claras de segurança, incluindo procedimentos para senhas fortes, autenticação de dois fatores, e acesso controlado a informações confidenciais;
d) **atualizações regulares**: manter os sistemas operacionais, aplicativos e softwares atualizados para evitar vulnerabilidades conhecidas;

e) **treinamento de funcionários**: conscientizar os colaboradores sobre as melhores práticas de segurança cibernética para evitar ataques de phishing e outras técnicas de engenharia social;
f) **backup e recuperação de dados**: realizar backups regulares e armazená-los em locais seguros para garantir a recuperação dos dados em caso de incidentes de segurança;
g) **criptografia**: utiliza criptografia para proteger dados confidenciais, garantindo que mesmo se forem interceptados, não possam ser acessados sem a chave adequada;
h) **auditorias de segurança**: realizar auditorias periódicas para identificar e corrigir possíveis vulnerabilidades e garantir que as políticas de segurança sejam seguidas adequadamente.

3.4 Qual é o papel dos governos e das agências de aplicação da lei na prevenção e investigação de crimes cibernéticos, incluindo a cooperação internacional entre países?

O papel dos governos e das agências de aplicação da lei na prevenção e investigação de crimes cibernéticos é de extrema importância na era digital em que vivemos. Algumas das principais responsabilidades incluem a prevenção, onde os governos devem desenvolver políticas e estratégias para proteger infraestruturas críticas, redes governamentais e sistemas de informação contra ameaças cibernéticas. Isso envolve o estabelecimento de regulamentações e padrões de segurança cibernética que as empresas e organizações devem seguir e as agências de aplicação da lei são responsáveis por investigar e perseguir criminosos cibernéticos. Isso inclui a coleta de evidências digitais, identificação dos responsáveis e rastreamento de atividades maliciosas na Internet. Os governos devem promover a educação em segurança cibernética para os cidadãos, empresas e organizações, incentivando a adoção de melhores práticas de segurança e a prevenção de ameaças. Eles também devem criar e atualizar leis relacionadas à segurança cibernética e crimes eletrônicos, garantindo que haja mecanismos legais eficazes para processar criminosos e proteger as vítimas.

A segurança cibernética é um desafio em constante evolução, e a cooperação internacional é fundamental para enfrentar as ameaças cibernéticas em escala global. A troca de conhecimento, experiências e informações entre países é essencial para construir uma defesa mais robusta contra-ataques cibernéticos.

3.5 Quais são as possíveis implicações éticas e legais do uso de técnicas de hacking por empresas de segurança da informação e pesquisadores de segurança para encontrar e corrigir vulnerabilidades em sistemas e redes de computadores?

O uso de técnicas de hacking por empresas de segurança da informação e pesquisadores de segurança, conhecido como "hacking ético" ou "teste de penetração", pode trazer várias implicações éticas e legais. Embora essas práticas sejam realizadas com o objetivo de melhorar a segurança dos sistemas e redes, é essencial ter cuidado para evitar violações de privacidade e danos não intencionais. Realizar testes de penetração sem a devida autorização pode ser considerado ilegítimo em algumas jurisdições e sujeito a sanções legais. É crucial obter permissão por escrito dos proprietários ou responsáveis pelos sistemas antes de realizar qualquer tipo de teste de segurança, garantindo que todas as partes envolvidas estejam cientes do processo. Testes de penetração podem envolver o acesso a dados confidenciais e pessoais, o que requer um cuidadoso manuseio e proteção dessas informações para evitar violações de privacidade. Os hackers éticos devem seguir um código de ética e conduta profissional, agindo com integridade e respeito aos princípios éticos durante suas atividades. Para mitigar essas implicações éticas e legais, é essencial seguir diretrizes éticas reconhecidas, como as definidas pela EC-Council (Conselho Internacional de Consultores Certificados de Ética) ou organizações semelhantes. Além disso, empresas de segurança e pesquisadores devem colaborar com os proprietários dos sistemas e seguir as leis e regulamentos locais relacionados à segurança da informação.

3.6 Hackers e a segurança cibernética: uma visão geral para grandes polos

Nos últimos anos, a crescente dependência da sociedade em relação à tecnologia trouxe consigo um aumento nos riscos relacionados à segurança cibernética. A ameaça constante de ataques cibernéticos e violações de dados coloca em destaque a importância de fortalecer as

defesas digitais de empresas e governos. Uma abordagem inovadora e eficaz para enfrentar esses desafios é a colaboração com hackers, profissionais habilidosos que, quando orientados para o bem, podem se tornar valiosos aliados na busca pela segurança cibernética.

Os hackers são indivíduos que possuem habilidades avançadas em informática e segurança cibernética, mas seu papel na sociedade é frequentemente mal compreendido devido às atividades ilegais de alguns deles. Existem diferentes categorias de hackers, incluindo os hackers éticos (white hats) que buscam identificar e corrigir vulnerabilidades de segurança, e os hackers maliciosos (black hats) que exploram essas vulnerabilidades para fins ilícitos.

A evolução dos hackers ao longo do tempo é marcada por sua adaptação às mudanças tecnológicas e às demandas do ambiente digital. Os desafios de segurança cibernética enfrentados por empresas e governos incluem ameaças como ataques de ransomware, vazamento de dados e intrusões em infraestruturas críticas.

3.6.1 Hackers éticos e sua contribuição para a segurança cibernética

Os hackers éticos desempenham um papel fundamental na identificação e correção de vulnerabilidades antes que sejam exploradas por atores maliciosos. Sua abordagem proativa ajuda a evitar brechas de segurança e reduzir o risco de ataques cibernéticos. Um exemplo notável é o programa de recompensa por bugs, no qual empresas oferecem incentivos financeiros a hackers éticos que descobrem e relatam vulnerabilidades.

Vários casos de sucesso demonstram como hackers éticos têm desempenhado um papel vital na proteção de sistemas. Por exemplo, em 2017, um hacker ético impediu um ataque de ransomware em larga escala ao encontrar um "interruptor de matança" no código malicioso.

3.6.2 Colaboração entre hackers e organizações: benefícios e desafios

A colaboração entre hackers éticos e organizações oferece uma série de benefícios. Primeiramente, permite a identificação proativa de vulnerabilidades, o que reduz o risco de

violações de segurança. Além disso, a experiência e o conhecimento dos hackers podem enriquecer as estratégias de segurança interna.

No entanto, essa colaboração não está isenta de desafios. Questões éticas, legais e de confidencialidade precisam ser abordadas de maneira cuidadosa. Por exemplo, hackers éticos podem inadvertidamente expor informações sensíveis durante suas investigações.

3.6.3 Estratégias para integrar hackers éticos em equipes de segurança

A integração eficaz de hackers éticos em equipes de segurança requer uma abordagem bem definida. O recrutamento e a seleção devem considerar a ética, as habilidades técnicas e a capacidade de colaborar com outras equipes. O treinamento contínuo é essencial para manter os hackers atualizados sobre as últimas ameaças e técnicas de segurança.

Estabelecer diretrizes claras e acordos de trabalho é crucial para garantir a colaboração bem-sucedida entre hackers e organizações. Isso inclui definir os limites das atividades dos hackers, a comunicação transparente e a proteção das informações sensíveis.

3.6.4 Resultados e impactos da colaboração

A colaboração entre hackers éticos e organizações tem demonstrado resultados significativos na melhoria da segurança cibernética. Empresas que adotaram essa abordagem observaram uma redução nas vulnerabilidades exploráveis, uma resposta mais rápida a ameaças emergentes e uma maior confiança dos clientes.

Além dos benefícios imediatos, a colaboração também tem impactos mais amplos na segurança da informação em escala global. A promoção de uma cultura de segurança cibernética e a conscientização pública são impulsionadas pela demonstração de que hackers podem ser agentes do bem.

A colaboração entre hackers e organizações representa uma abordagem inovadora para melhorar a segurança cibernética. Ao adotar hackers éticos como agentes do bem, empresas e

governos podem fortalecer suas defesas digitais, proteger informações sensíveis e contribuir para a construção de um ambiente digital mais seguro.

4 BILHÕES DENTRE BILHÕES: INFORMAÇÃO E PODER.

4.1 Como a informação se tornou uma das principais fontes de poder na nova era e como isso impacta a sociedade e a economia

4.1.1 O que é a Era da Informação?

A informação se tornou uma das principais fontes de poder nessa nova era devido ao imenso volume de dados disponíveis e graças as novas tecnologias de processamento desses dados e análise avançada. Em resumo, essa é a era da informação: “A era da informação é o atual período técnico e científico em que estamos inseridos, caracterizado pelo rápido surgimento e aprimoramento das tecnologias da informação e da comunicação. Esse processo faz com que a distância física entre os territórios deixe de ser um impeditivo para a conexão, criando assim um espaço organizado em redes em que há um intenso fluxo de informações, capitais, mercadorias e pessoas.” (BRASIL ESCOLA, [s.d.]).

4.1.2 Como a informação se tornou uma fonte de poder?

Nesse novo mundo digital, diversos fatores interconectados foram o motivo da informação ter se tornado uma das principais fontes de poder. Com a explosão da internet e das tecnologias digitais a informação se tornou amplamente acessível e disponível para muitas pessoas, diversos canais e plataformas fornecem acesso instantâneo a uma quantidade imensa de informação, o que também ajuda é a capacidade de compartilhamento, essa facilidade permite que as pessoas transmitam conhecimento e informação em nível global, não só nacional como em tempos passados. Através de tudo isso, empresas podem criar perfis totalmente personalizados para clientes. A influência, persuasão, competitividade e inovação também tem grande envolvimento nesse tipo de poder, pois além das estratégias de marketing digital que muitas vezes estão baseadas em comportamentos da psique humana. “Nesse sentido, a psicologia tende a apresenta-se como um elo fundamental entre o marketing e o advertising, em que se utiliza os princípios psicológicos para fins de direcionar da melhor forma, a produção empresarial para suprir alguma necessidade humana. Inclusive, na atualidade, o verdadeiro empreendedor está a procurar aplacar alguma necessidade inconsciente de seus clientes, bem

como produzir bens que prendam a atenção do consumidor e as tornem desejáveis, caso produzidas" (DAWSON, 2005, p. 64 apud SANT'ANNA, 2018). Aqueles que têm acesso a informações atualizadas e relevantes possuem uma vantagem competitiva significativa. A informação é essencial para a inovação, permitindo que empresas identifiquem novas oportunidades de negócio, antecipem tendências e adaptem-se às mudanças do mercado.

4.1.3 Como isso impacta a sociedade e a economia?

A Era da Informação modificou tanto as relações sociais como a forma de consumo. Por consequência, com esses novo padrões de consumo, influenciados pelas novas tecnologias digitais, que, na maioria das vezes, está tudo na palma de suas mãos, as empresas precisam chegar aos clientes de novas formas. "A grande novidade é que não é mais preciso ter um produto palpável para gerar uma montanha de dinheiro. O Facebook, por exemplo, que ocupa o quinto lugar no ranking de empresas mais valiosas da FORBES, sempre foi uma plataforma gratuita e, por muito tempo, não rendeu nada a seus proprietários." (FIA; GUEDES, 2019), o comércio eletrônico permite que as empresas alcancem clientes em todo o mundo, reduzindo as limitações geográficas e ampliando o mercado. Isso oferece oportunidades de crescimento para empresas de todos os tamanhos e impulsiona a concorrência e a eficiência no mercado. com essa "digitalização" das relações, as pessoas se conectam de maneiras mais rápidas e eficientes. As redes sociais, aplicativos de mensagens e plataformas de videoconferência facilitam a comunicação instantânea e global, encurtando as distâncias e permitindo interações em tempo real.

4.2 Quais são as principais estratégias utilizadas pelas empresas de tecnologia para coletar, analisar e utilizar grandes quantidades de dados e qual é o seu impacto na privacidade dos usuários?

4.2.1 O que é a coleta de dados?

As empresas de tecnologias utilizam diversas formas e jeitos de coletar e analisar grandes quantidade de dados. Isso permite que elas tomem decisões estratégicas, melhorem seus produtos e serviços e em vários casos, direcionem corretamente seu marketing e

publicidade, porém, há controvérsias. Muitas vezes essas práticas criam dúvidas e preocupações sobre a privacidade e como isso impacta a vida de seus usuários. “A coleta de dados é um processo voltado à captação de conteúdo estratégico que pode ser encontrado em ferramentas de análise, formulários e outros softwares que retenham essas informações. Esse processo tem a finalidade de garantir às empresas conhecer a fundo resultados de setores, do mercado, da percepção do consumidor e do desempenho do negócio de modo geral. Por mais que a coleta de dados possa parecer um evento extraordinário, trata-se apenas de uma atividade rotineira do cotidiano das empresas. Atualmente, os dados são considerados ativos extremamente valiosos em qualquer mercado, simplesmente porque podem traduzir os resultados das empresas e a percepção externa sobre produtos, serviços e marca.” (ROCKCONTENT; FERREIRA, 2020).

4.2.2 Que estratégias são essas e qual o impacto e as consequências na privacidade e vida dos usuários?

Através da big data; coleta passiva de dados; aprendizado de máquina e inteligência artificial, integração de dados de terceiros, e da venda e compartilhamento de informações, a coleta e análise de grandes quantidades de dados tornaram-se práticas comuns entre as empresas tecnológicas. Embora essas práticas possam melhorar a experiência do usuário, a falta de transparência e controle sobre a utilização dos dados pode resultar em violações de privacidade e riscos de segurança. Para proteger a privacidade dos usuários, várias regiões ao redor do mundo implementaram regulamentações de proteção de dados, como o GDPR na União Europeia e a LGPD no Brasil. Essas leis buscam garantir que as empresas tratem os dados dos usuários com responsabilidade, oferecendo maior transparência e opções de consentimento.

4.3 Como as estratégias de manipulação da informação são utilizadas para influenciar a opinião pública, a política e os negócios, e quais são as possíveis soluções para minimizar esse impacto negativo?

A manipulação da informação é uma prática que tem sido amplamente utilizada para influenciar a opinião pública, moldar narrativas políticas e afetar os negócios de diversas maneiras. Com o avanço das tecnologias de comunicação e o fácil acesso à informação, as estratégias de manipulação se tornaram mais sofisticadas e disseminadas, tornando-se um

desafio significativo para a sociedade. “A presença de propaganda e informações manipuladas em notícias e mídias sociais é uma ameaça à nossa democracia e à nossa capacidade de tomar decisões bem fundamentadas.”(CONJUR; QUEIROZ, 2017) Essas estratégias têm potencial para causar sérios danos à sociedade, minando a confiança nas instituições, prejudicando a tomada de decisões informadas e contribuindo para a desestabilização política e social. * Uma “fake news” não é uma simples “fake news”, se muito disseminada, pode causar danos irreversíveis em pessoas inocentes ou empresas.

Para combater a manipulação da informação e seus impactos negativos na opinião pública, na política e nos negócios, é essencial adotar uma abordagem abrangente e colaborativa. É necessário também educação em mídia e alfabetização digital, ou seja, investir em programas educacionais que promovam o pensamento crítico e ensinem as pessoas a avaliarem cuidadosamente as fontes de informação. Combater a disseminação de contas falsas e bots também é importante para evitar que a desinformação seja amplificada artificialmente, incentivar o público a questionar informações suspeitas, buscar fontes diversas e considerar diferentes perspectivas antes de formar uma opinião. O pensamento crítico ajuda a construir uma sociedade mais resiliente contra a manipulação da informação. Embora cada solução por si só não seja suficiente, a combinação de todas essas estratégias é essencial para enfrentar efetivamente a manipulação da informação.

5 ONDE NÓS ESTAMOS NO TABULEIRO

5.1 Evolução da informação.

A evolução da informação como fonte de poder e as implicações na privacidade dos usuários têm sido amplamente discutidas. Como afirmado por Manuel Castells em seu livro "A Sociedade em Rede", "a informação é poder e quem controla a informação tem poder" (CASTELLS, 1996). Nesse sentido, o advento da era digital e a interconectividade global têm aumentado a importância da cibersegurança na proteção das informações sensíveis.

As ciberguerras têm impacto direto na privacidade dos usuários e na liberdade de expressão online. Conforme mencionado por Bruce Schneier em seu livro "Data and Goliath", "os governos e outras organizações podem usar tecnologia para espionar cidadãos e restringir a liberdade de expressão" (SCHNEIER, 2015). A disseminação de táticas cibernéticas por governos autoritários tem levantado preocupações sobre a violação da privacidade e a censura online.

5.2 Como é para os usuários comuns, empresas e governos os desafios da cibersegurança.

Para os usuários comuns, os desafios da segurança cibernética são cada vez mais evidentes. A proliferação de ameaças de malware, phishing e roubo de identidade coloca em risco a segurança e a privacidade dos dados pessoais. Como mencionado no website do, "os usuários devem adotar medidas de proteção, como a utilização de senhas fortes e a atualização regular dos softwares de segurança" (DEPARTMENT OF HOMELAND SECURITY, 2021).

As empresas e governos têm um papel fundamental na promoção da segurança cibernética. De acordo com o Relatório de Segurança Cibernética da União Europeia, "as empresas devem investir em infraestrutura segura e educar seus funcionários sobre boas práticas de segurança" (EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2020). Além disso, os governos estão implementando políticas e regulamentações para incentivar a segurança

cibernética, como destacado pelo National Institute of Standards and Technology (NIST) dos Estados Unidos em suas diretrizes de segurança cibernética (NIST, 2020).

5.3 Mudança de pensamento e a conscientização do poder da informação.

A conscientização sobre a importância da segurança cibernética está mudando a forma como as pessoas pensam sobre a segurança online. Conforme mencionado por Kevin Mitnick em seu livro "The Art of Invisibility", "a segurança cibernética é agora uma preocupação primordial, e os usuários estão cada vez mais cautelosos em relação à proteção de seus dados pessoais" (MITNICK, 2017). Essa mudança de pensamento impulsiona o desenvolvimento de tecnologias e soluções mais seguras.

Em suma, a informação se tornou uma fonte de poder na era digital, e a segurança cibernética desempenha um papel crucial na proteção da privacidade dos usuários e na liberdade de expressão online. As ciberguerras, os desafios para os usuários comuns e os esforços das empresas e governos na promoção da segurança cibernética são questões fundamentais discutidas em diversas obras e referências. A mudança de pensamento em relação à segurança online tem implicações significativas na sociedade e no futuro da tecnologia. Como afirmado por Tim Maurer em seu livro "Cyber Mercenaries: The State, Hackers, and Power", "a segurança cibernética está remodelando a forma como pensamos sobre a segurança, afetando todos os aspectos de nossas vidas, desde a proteção de nossos dados pessoais até a segurança de infraestruturas críticas" (MAURER, 2018).

Essa mudança de pensamento também tem impacto nas políticas públicas e na governança da internet. Conforme ressaltado pelo Internet Governance Project, um projeto de pesquisa colaborativo, "a segurança cibernética está se tornando uma prioridade para governos e organizações internacionais, que buscam estabelecer normas e regulamentações para promover uma internet mais segura e confiável" (INTERNET GOVERNANCE PROJECT, 2021).

Além disso, a preocupação com a segurança cibernética está impulsionando a inovação tecnológica. Como apontado por Larry Clinton, presidente da Internet Security Alliance, "a

segurança cibernética está se tornando um diferencial competitivo para as empresas, incentivando o desenvolvimento de soluções avançadas, como a inteligência artificial e a criptografia de ponta" (CLINTON, 2020).

No entanto, é fundamental equilibrar a segurança cibernética com a preservação da privacidade e da liberdade de expressão. Como destacado pela Electronic Frontier Foundation, uma organização sem fins lucrativos que defende os direitos digitais, "é essencial encontrar um equilíbrio entre a segurança cibernética e os direitos individuais, evitando medidas excessivamente invasivas que possam comprometer a privacidade e a liberdade na internet" (ELETRONIC FRONTIER FOUDATION, 2021).

Em conclusão, a cibersegurança é um tema crucial na era digital, em que a informação se tornou uma fonte de poder. As ciberguerras, os desafios enfrentados pelos usuários comuns e os esforços das empresas e governos para promover uma internet mais segura são tópicos amplamente discutidos em literatura e referências especializadas. A mudança de pensamento em relação à segurança online está moldando a sociedade e o futuro da tecnologia, com implicações tanto positivas quanto desafiadoras que exigem um equilíbrio adequado entre segurança, privacidade e liberdade.

6 ARMANDO ARMADILHAS

6.1 Quais são os tipos mais comuns de armadilhas que os usuários podem encontrar na internet?

Os ataques mais comuns que ocorrem na internet são:

a) **backdoor**: ou porta dos fundos, é um ataque muito popular, devido ao seu sistema de funcionamento, que vem através de instalação pelos próprios desenvolvedores do sistema e dos apps, dando acesso ao seu sistema de forma remota, permitindo as instalações de softwares maliciosos, manipulação de arquivos, execução de programas, e até mesmo o envio de e-mails (Backdoor não é um tipo de ataque, é uma "porta de volta");
b) **phishing**: tem como objetivo utilizar a engenharia social, ou seja, a confiança do usuário, o atacante se passa por uma instituição legítima, e pede para você preencher seus dados, com essa manipulação a sua principal função é o roubo de dados pessoais, como senhas;
c) **spoofing**: está relacionado com a falsificação de endereços de IP, de DNS e de e-mails, os criminosos simulam uma fonte de IP confiável, editar o cabeçalho de um e-mail para parecer ser legítimo, ou modificar o DNS a fim de redirecionar um determinado nome de domínio para outro endereço IP, esse ataque tem como principal função a falsificação de identidade;
d) **ataque DDos**: é um ataque em que o atacante utiliza diversas máquinas tenta inoperar um acessando um site ou serviço específico causando a uma sobrecarga desse site, e posteriormente tirando-o do ar, esse ataque tem como principal função a negação e a inutilização doesse serviço.

6.2 Quais implicações da coleta e uso de dados pessoais pelos aplicativos e serviços online?

A coleta e uso de dados pessoais por aplicativos e serviços online têm várias implicações, algumas das quais podem ser positivas, mas também existem preocupações

significativas relacionadas à privacidade e à segurança. Aqui estão algumas das principais implicações positivas:

a) **melhoria dos serviços**: a coleta de dados pessoais permite que os desenvolvedores entendam melhor o comportamento e as preferências dos usuários, o que pode levar a melhorias nos produtos e serviços oferecidos. Isso pode resultar em experiências mais personalizadas e eficazes;
b) **publicidade direcionada**: os dados coletados podem ser usados para segmentar anúncios com base nos interesses e comportamentos dos usuários, o que pode tornar a publicidade mais relevante para os consumidores e aumentar a eficácia das campanhas publicitárias;
c) **inovação**: a análise de grandes conjuntos de dados pessoais pode levar a insights valiosos e a inovações em diversas áreas, como medicina, transporte e educação.

Porém também há implicações negativas como:

a) **violação de privacidade**: a coleta de dados pessoais pode violar a privacidade dos usuários, especialmente se os dados forem compartilhados sem o seu consentimento adequado ou se forem usados de maneira inadequada;
b) **risco de roubo de identidade**: dados pessoais, como números de cartão de crédito e informações de identificação, podem ser alvo de hackers e criminosos cibernéticos, resultando em roubo de identidade e fraude;
c) **vigilância em massa**: governos e empresas podem usar a coleta de dados para fins de vigilância em massa, o que pode prejudicar as liberdades civis e a privacidade dos cidadãos;
d) **discriminação**: o uso de dados pessoais para tomar decisões automatizadas, como concessão de crédito ou contratação, pode resultar em discriminação injusta com base em características protegidas por lei, como raça, gênero e orientação sexual;
e) **vazamentos de dados**: mesmo empresas bem-intencionadas podem sofrer vazamentos de dados, expondo informações pessoais dos usuários e causando danos à reputação das empresas e à segurança dos usuários;

f) **desigualdade digital**: aqueles que não têm acesso a dispositivos ou serviços online podem ficar excluídos de muitas oportunidades e serviços digitais, criando uma desigualdade digital.

Para lidar com essas implicações, muitos países têm implementado regulamentações de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei de Privacidade do Consumidor da Califórnia (CCPA) nos Estados Unidos. Essas leis visam proteger os direitos dos indivíduos em relação aos seus dados pessoais e garantir maior transparência e controle sobre como esses dados são coletados e utilizados. Além disso, é importante que os usuários estejam cientes de suas opções de privacidade e façam escolhas informadas ao usar aplicativos e serviços online.

7 DESMONTANDO ARMADILHAS

7.1 Como a alfabetização digital pode ajudar os usuários a identificarem e evitar armadilhas on-line e quais são os desafios da educação digital na era da informação

A alfabetização digital desempenha um papel crucial na capacitação dos usuários para identificar e evitar armadilhas online. Ela pode ajudar nesse processo, bem como os desafios da educação digital na era da informação.

7.1.1 A alfabetização digital como conscientizadora dos usuários sobre as armadilhas on-line

A alfabetização ensina aos usuários habilidades essenciais para reconhecer sinais de possíveis armadilhas on-line, como:

a) **conscientização sobre phishing**: os usuários aprendem a identificar e-mails, mensagens ou sites suspeitos que buscam obter informações pessoais ou financeiras, e são orientados a não clicar em links desconhecidos ou fornecer informações confidenciais;
b) **gerenciamento de privacidade**: o ensino digital abrange o conhecimento de configurações de privacidade e segurança, permitindo que os usuários protejam suas informações pessoais e restrinjam o acesso não autorizado a seus dados.

Ela também ajuda os usuários a evitarem ataques cibernéticos, como malware e ransomware, através do reconhecimento de práticas inseguras, onde os usuários são instruídos a evitar práticas inseguras, como baixar arquivos de fontes não confiáveis, abrir anexos de e-mails suspeitos ou clicar em pop-ups desconhecidos.

7.1.2 Desafios da educação digital na era da informação:

Embora a alfabetização seja fundamental, existem desafios que precisam ser superados:

a) **velocidade das mudanças tecnológicas**: a rápida evolução da tecnologia torna desafiador manter-se atualizado sobre os mais recentes riscos e armadilhas on-line. É necessário um esforço contínuo para atualizar os currículos de alfabetização digital e garantir que eles acompanhem as tendências e avanços tecnológicos;
b) **disparidades no acesso à tecnologia**: nem todos têm acesso igualitário à tecnologia e à internet, o que cria uma lacuna digital. Garantir que o ensino digital esteja acessível a todos os grupos socioeconômicos é essencial para combater armadilhas on-line;
c) **habilidades de discernimento**: identificar armadilhas e informações enganosas exige habilidades críticas de pensamento, discernimento e avaliação. A educação digital precisa desenvolver essas habilidades nos usuários para que eles possam tomar decisões informadas e evitar armadilhas;
d) **sobrecarga de informações**: na era da informação, os usuários estão expostos a uma quantidade enorme de dados e conteúdos on-line. Ensinar os usuários a filtrarem informações relevantes e confiáveis é um desafio significativo.

A alfabetização digital desempenha um papel crucial na proteção dos usuários on-line, capacitando-os a identificar e evitar armadilhas. No entanto, superar os desafios da educação digital na era da informação requer esforços contínuos para atualização, acesso igualitário, desenvolvimento de habilidades de discernimento e gerenciamento da sobrecarga de informações.

7.2 Quais são as técnicas de investigações utilizadas pelos especialistas em segurança da informação para descobrir e desmontar armadilhas on-line como malware, phishing e engenharia social?

As tecnologias mais utilizadas pelos especialistas para descobrir e desmontar as armadilhas on-line de forma técnica são:

a) **análise de malware**: os especialistas em segurança utilizam ambientes controlados, como "sandboxes" (ambientes isolados) para executar o malware

e analisar seu comportamento através do seu código fonte. Isso ajuda a identificar sua funcionalidade, métodos de propagação e possíveis contramedidas;

b) **engenharia reversa**: os especialistas desmontam e analisam o código-fonte do malware para entender sua estrutura interna, algoritmos e técnicas de evasão. Isso permite que eles desenvolvam soluções para detecção e remoção do malware;
c) **análise de tráfego**: monitorar e analisar o tráfego de rede é uma técnica eficaz para identificar atividades suspeitas. Os especialistas em segurança observam as comunicações entre sistemas e procuram padrões incomuns que possam indicar a presença de malware ou atividades maliciosas;
d) **forense digital**: a investigação forense digital é usada para coletar, preservar e analisar evidências digitais relacionadas a incidentes de segurança. Isso pode incluir a análise de logs do sistema, registros de eventos, arquivos temporários e outros dados relevantes para identificar a origem e a extensão de uma ameaça.

Essas são algumas das técnicas que são comumente usadas pelos especialistas em segurança da informação. É importante notar que a segurança cibernética é um campo em constante evolução, e os especialistas estão sempre se adaptando e desenvolvendo novas técnicas para enfrentar ameaças emergentes.

7.3 Como usuários podem identificar sinais de alertas em sites e aplicativos suspeitos?

Identificar sinais de alerta em sites e aplicativos suspeitos é essencial para proteger-se contra fraudes, golpes e violações de segurança. Aqui estão algumas dicas que os usuários podem seguir para identificar possíveis ameaças:

a) **verificar o URL e SSL**: é de suma importância analisar o URL do site para ter certeza de que ele é correto e legítimo. Além disso, certificar de que o endereço comece com "https://" em vez de "http://" e procurar pelo símbolo de um cadeado na barra de endereços, o que indica que a conexão é segura e criptografada;

b) **design e layout**: ficar atento ao design e ao layout do site ou aplicativo é imprescindível, pois sites maliciosos podem ter aparência amadora, com imagens de baixa qualidade, erros gramaticais, fontes estranhas ou design desorganizado;
c) **solicitação de informações sensíveis**: desconfiar de sites ou aplicativos que solicitem informações pessoais sensíveis logo de início, especialmente antes de você estabelecer a confiança com o serviço é essencial. Informações como senhas, números de cartão de crédito ou documentos de identificação devem ser fornecidas apenas em sites confiáveis e seguros;
d) **anúncios e redirecionamentos excessivos**: caso o site ou aplicativo exibir uma quantidade excessiva de anúncios ou redirecioná-lo constantemente para outras páginas suspeitas, é um sinal de alerta;
e) **política de privacidade e termos de uso**: a verificação se o site possui uma política de privacidade clara e detalhada, bem como termos de uso deve ser feita já que a ausência dessas informações ou redação confusa pode indicar que o site não é legítimo;
f) **revisões e classificações**: deve ser feita uma busca por revisões e classificações do site ou aplicativo em questão. Pesquisar opiniões de outros usuários pode fornecer insights valiosos sobre a confiabilidade e segurança do serviço;
g) **confirmação da identidade da empresa ou organização**: caso o site ou aplicativo represente uma empresa ou organização conhecida, deve ser feita uma verificação se há informações de contato, endereço físico e outras provas de sua existência e autenticidade;
h) **ofertas duvidosas e tendenciosas**: desconfiar de ofertas que pareçam duvidosas e tendenciosas é sempre necessário porque golpistas frequentemente utilizam iscas tentadoras para atrair usuários desavisados;
i) **mensagens de alerta e aviso**: em caso de recebimento de mensagens de alerta ou aviso durante a navegação no site, especialmente aquelas que solicitam ação imediata ou informações pessoais, é fundamental a cautela. Se porventura isso ocorrer, consultar fontes adicionais ou fazer contato ao suporte oficial da empresa para verificar a veracidade dessas mensagens é essencial.

7.4 Quais são as ferramentas e tecnologias disponíveis para detectar e prevenir ataques cibernéticos e como os usuários podem usá-las de forma eficaz?

A utilização de antivírus, como o kaspersky, que utiliza algumas camadas de segurança para a proteção contra ransoc e ransomware. Firewall, controla o fluxo de dados através de sua rede de internet, permitindo ou não alguns pacotes de dados. Protocolo de segurança e a utilização de criptografia, e autenticação de dois fatores que é uma camada adicional de segurança que requer duas formas de verificação para acessar uma conta. Isso geralmente envolve uma combinação de senha e um fator adicional, como um código enviado por SMS, um token físico ou um aplicativo de autenticação

7.5 Como as empresas e os governos estão trabalhando juntos para combater a cibercriminalidade e quais são as possíveis implicações disso para a privacidade e a segurança do usuário?

A colaboração entre empresas e governos é essencial para combater a cibercriminalidade de maneira eficaz. Em ocasiões de:

a) **compartilhamento de inteligência**: empresas e governos compartilham informações sobre ameaças cibernéticas e táticas utilizadas por hackers e grupos criminosos. Essa troca de inteligência permite que ambas as partes sejam mais proativas na identificação e mitigação de riscos de segurança cibernética;
b) **denúncia e cooperação em investigações**: empresas frequentemente notificam agências governamentais sobre ataques cibernéticos, e os governos, por sua vez, fornecem suporte para investigar e responsabilizar os culpados. Isso pode incluir a cooperação entre equipes de resposta a incidentes cibernéticos e agências de aplicação da lei;
c) **regulação e legislação**: os governos desenvolvem leis ou atualizam elas e regulamentos relacionados à segurança cibernética e à privacidade para garantir que as empresas adotem práticas adequadas de proteção de dados e infraestrutura. As empresas, por sua vez, devem cumprir essas normas e

colaborar com as autoridades em questões de conformidade e relatórios de incidentes;

d) **participação em iniciativas e grupos de trabalho**: tanto empresas quanto governos podem fazer parte de iniciativas e grupos de trabalho relacionados à cibersegurança. Esses fóruns permitem que compartilhem melhores práticas, desenvolvam estratégias conjuntas e trabalhem em prol de objetivos comuns para combater a cibercriminalidade.

No entanto, essa colaboração também pode ter implicações para a privacidade e a segurança do usuário, que devem ser consideradas e equilibradas cuidadosamente:

a) **privacidade dos usuários**: o compartilhamento de informações entre empresas e governos pode levantar preocupações com a privacidade dos usuários. É importante garantir que os dados pessoais sejam tratados com cuidado e que o acesso a essas informações seja estritamente controlado para evitar abusos;
b) **segurança dos dados compartilhados:** a troca de informações sobre ameaças cibernéticas deve ser realizada de maneira segura, para evitar que dados sensíveis caiam em mãos erradas. As empresas e os governos devem adotar medidas de segurança robustas para proteger essas informações confidenciais;
c) **uso responsável de dados:** as informações compartilhadas devem ser utilizadas apenas para fins legítimos de combate à cibercriminalidade e não devem ser exploradas para outros fins sem o consentimento apropriado.

8 ENGENHARIA SOCIAL COMO ARMA DE PERSUASÃO

8.1 Como a engenharia social é utilizada por hackers e cibercriminosos para obter informações sensíveis dos usuários, como senhas e dados bancários, e como os usuários podem se proteger contra esses ataques?

A engenharia social é uma técnica psicológica que visa manipular e enganar pessoas para que elas revelem informações confidenciais, como senhas, dados bancários ou informações pessoais. Hackers e cibercriminosos frequentemente utilizam essa abordagem porque é mais prático explorar as fraquezas humanas do que tentar contornar sistemas de segurança complexos. Aqui estão algumas maneiras como a Engenharia Social é usada por eles e como os usuários podem se proteger:

8.1.1 Dicas para proteção de ataques de engenharia social:

a) **desconfiar de solicitações de informações pessoais**: é extremamente importante não fornecer informações confidenciais, como senhas, números de cartões de crédito ou informações bancárias, por telefone, e-mail ou mensagens;
b) **verificação da fonte**: verificar a autenticidade da pessoa ou organização que está solicitando informações antes de fornecer qualquer dado é uma ação essencial assim como usar informações de contato oficiais;
c) **atenção a URLs**: verificar cuidadosamente os URLs antes de clicar em qualquer link porque sites de phishing frequentemente usam endereços semelhantes aos originais, mas com pequenas variações;
d) **cautela com anexos e downloads**: não abrir anexos ou baixar arquivos de fontes não confiáveis, já que eles podem conter malware;
e) **continuar procurando informações**: estudar sobre os tipos mais recentes de ataques de Engenharia Social e compartilhar essas informações com amigos e familiares para que todos fiquem alertas;
f) **configuração da autenticação de dois fatores (2FA)**: usar autenticação de dois fatores é indispensável, pois ela adiciona uma camada extra de segurança;

g) **controle das informações online**: limitar a quantidade de informações pessoais que você compartilha nas redes sociais e em outros sites é importante para evitar que atacantes possam se aproveitar de informações pessoais.

A prevenção sempre é a melhor abordagem. Se informar e ter atenção a possíveis tentativas de engenharia social pode ajudar a reduzir a probabilidade de cair em golpes desse estilo.

8.2 Quais são os métodos mais comuns de engenharia social, como phishing, tailgating e quais são os possíveis danos que esses ataques podem causar às empresas e indivíduos?

Existem vários métodos de engenharia social que são comuns entre hackers e cibercriminosos. Alguns dos mais conhecidos incluem:

a) **phishing**: é um método em que os criminosos enviam e-mails ou mensagens falsas que parecem ser de fontes confiáveis, como bancos, empresas ou colegas de trabalho. Esses e-mails geralmente solicitam informações confidenciais, como senhas, números de cartões de crédito ou informações bancárias. Os danos resultantes do phishing podem incluir roubo de identidade, acesso não autorizado a contas e perda financeira;
b) **spear phishing**: semelhante ao phishing, porém mais direcionado. Os criminosos pesquisam sobre a vítima e personalizam a mensagem para torná-la mais convincente. Isso pode incluir informações pessoais ou de trabalho da vítima. Os danos podem ser os mesmos do phishing, mas a probabilidade de sucesso é maior devido à personalização;
c) **whaling**: uma forma mais avançada de phishing que se concentra em alvos de alto nível, como executivos de empresas. Os criminosos buscam obter informações sensíveis ou acesso a sistemas corporativos confidenciais;
d) **tailgating (Piggybacking)**: envolve um criminoso seguindo um funcionário legítimo de uma empresa em um local seguro, como um escritório, onde não têm permissão. Isso pode permitir que eles acessem sistemas ou informações

confidenciais. Os danos podem incluir acesso não autorizado a informações corporativas e sistemas;

e) **quid pro quo**: nesse método, os criminosos oferecem algo em troca das informações da vítima. Isso pode ser algo como suporte técnico falso ou ofertas especiais. Os danos podem variar de roubo de informações pessoais a comprometimento de sistemas;
f) **pretexting**: aqui, os criminosos inventam uma história ou um pretexto para obter informações. Eles podem se passar por representantes de empresas ou autoridades para enganar as vítimas a fornecer detalhes pessoais. Os danos podem incluir roubo de identidade e acesso não autorizado a contas;
g) **engenharia social baseada em relacionamento**: os criminosos constroem relacionamentos falsos com as vítimas, ganhando sua confiança ao longo do tempo. Isso pode permitir o acesso a informações confidenciais. Os danos podem ser amplos, incluindo roubo de informações pessoais, financeiras ou corporativas;
h) **engenharia social online**: os cibercriminosos também exploram as redes sociais e outras informações online para criar perfis detalhados das vítimas, tornando seus ataques mais convincentes.

Os danos causados por esses ataques podem variar de perda financeira e roubo de identidade a comprometimento de sistemas corporativos e violações de dados. Empresas podem sofrer impactos significativos, como perda de propriedade intelectual, danos à reputação e possíveis ações judiciais. Indivíduos podem enfrentar prejuízos financeiros, perda de privacidade e dificuldades em recuperar suas identidades após um ataque bem-sucedido de engenharia social.

Portanto, a conscientização, a educação e a adoção de práticas de segurança sólidas são essenciais para proteger tanto empresas quanto indivíduos contra esses tipos de ataques.

8.3 Como as empresas e organizações estão se preparando para lidar com a ameaça da engenharia social, por meio de treinamentos de conscientização, políticas de segurança e tecnologias avançadas, e quais são os desafios para implementar essas medidas de segurança

Compreendendo a gravidade das ameaças representadas pela engenharia social, empresas e organizações estão adotando uma abordagem proativa para se protegerem. Essa preparação envolve a implementação de treinamentos de conscientização, políticas de segurança e o uso de tecnologias avançadas.

8.3.1 Treinamentos de conscientização para os colaboradores da organização

Os treinamentos de conscientização têm sido uma ferramenta crucial na capacitação dos funcionários para identificar e resistir a ataques de engenharia social. Esses programas educam os colaboradores sobre os diferentes tipos de ataques, ensinam como identificar sinais de manipulação e fornecem orientações sobre como reagir de maneira segura. Ao aumentar a conscientização sobre os perigos da engenharia social, as empresas capacitam seus funcionários a se tornarem uma linha de defesa eficaz.

As abordagens de treinamento podem variar desde palestras presenciais até cursos online interativos. Além disso, a realização de simulações de ataques de engenharia social, como testes de phishing controlados, permite que os funcionários pratiquem suas habilidades de detecção e reação em um ambiente seguro.

Além de educar os funcionários sobre a detecção e resistência a ataques de engenharia social, as empresas estão investindo em treinamentos específicos para evitar cair em golpes. Esses treinamentos visam capacitar os colaboradores a identificarem técnicas de manipulação, compreender os sinais de alerta e tomar decisões informadas para proteger suas informações e os ativos da organização.

a) **técnicas de reconhecimento**: os treinamentos ensinam os funcionários a reconhecerem sinais comuns de engenharia social, como solicitações urgentes de informações confidenciais, pedidos de transferência de fundos sem verificação ou ameaças de consequências negativas;

b) **verificação de identidade**: os funcionários são orientados a sempre verificar a identidade da pessoa que está solicitando informações ou ação. Isso pode envolver a confirmação através de canais alternativos ou a busca de autorização de superiores;
c) **gerenciamento de informações pessoais**: treinamentos enfatizam a importância de manter informações pessoais e corporativas seguras. Os colaboradores são instruídos a evitar compartilhar dados sensíveis, como senhas, por telefone ou e-mail, e a utilizar métodos seguros de comunicação;
d) **simulações de ataques**: através de simulações de ataques de phishing, os funcionários têm a oportunidade de vivenciar situações de engenharia social de forma controlada. Isso os ajuda a praticar suas habilidades de discernimento e reação em um ambiente seguro;
e) **educação sobre técnicas de engenharia social**: os treinamentos oferecem insights detalhados sobre as táticas de engenharia social, destacando como os agressores podem explorar fraquezas emocionais e psicológicas para obter informações. Isso permite que os funcionários se tornem mais resistentes a manipulações.

Esses treinamentos não apenas ajudam os funcionários a evitarem cair em golpes de engenharia social, mas também promovem uma cultura de segurança cibernética na organização. A conscientização e o comprometimento individuais se combinam para fortalecer a postura de segurança como um todo.

8.3.2 Políticas de segurança essenciais para preservação e continuação da segurança da informação na empresa

A implementação de políticas de segurança sólidas é um pilar fundamental na estratégia das empresas para mitigar os riscos associados à engenharia social. Essas políticas estabelecem diretrizes claras para a proteção de informações confidenciais, o uso responsável da tecnologia e a promoção de uma cultura organizacional focada na segurança cibernética.

a) **política de autenticação e autorização**: estabelecimento de procedimentos rigorosos para autenticação de usuários, incluindo senhas fortes e autenticação multifator, a fim de impedir acessos não autorizados.
b) **política de gerenciamento de senhas**: diretrizes para a criação, armazenamento seguro e atualização regular de senhas, com ênfase na importância de não compartilhar senhas com terceiros.
c) **política de uso de dispositivos móveis**: definição de regras para o uso seguro de dispositivos móveis, incluindo a proteção contra perda ou roubo, uso de redes Wi-Fi públicas e instalação de aplicativos confiáveis.
d) **política de comunicações seguras**: instruções sobre como compartilhar informações sensíveis de maneira segura, incluindo a preferência por métodos criptografados e canais de comunicação aprovados.

8.3.3 Tecnologias para mitigação da engenharia social

As tecnologias desempenham um papel crucial na detecção e prevenção de ataques de engenharia social. A combinação de soluções tecnológicas avançadas com políticas de segurança eficazes aumenta significativamente a capacidade das empresas de se protegerem contra essa ameaça. Algumas das tecnologias para diminuir o uso de engenharia social são:

a) **autenticação multifator (AMF)**: a AMF requer que os usuários forneçam duas ou mais formas de autenticação antes de acessar sistemas ou informações sensíveis. Isso adiciona uma camada adicional de segurança, tornando mais difícil para os agressores obterem acesso não autorizado;
b) **ferramentas de detecção de phishing**: softwares de detecção de phishing analisam e filtram e-mails em busca de características suspeitas, como URLs falsas ou anexos maliciosos. Eles ajudam a identificar e-mails fraudulentos antes que os funcionários se tornem vítimas;
c) **análise comportamental**: essa tecnologia monitora o comportamento dos usuários para identificar padrões anômalos de atividade. Se um usuário começar a agir de maneira incomum, como acessar arquivos não autorizados ou fazer transferências financeiras suspeitas, a tecnologia pode acionar alertas;

d) **simulações de ataques**: as empresas estão recorrendo a simulações de ataques de engenharia social como uma forma de treinamento contínuo. Essas simulações envolvem o envio de e-mails ou mensagens falsas para testar a capacidade dos funcionários de identificar e relatar ataques.

A combinação dessas políticas de segurança e tecnologias avançadas cria uma abordagem abrangente de defesa contra a engenharia social. No entanto, a implementação dessas medidas não está isenta de desafios.

8.3.4 Desafios para implementar essas medidas de segurança

A implementação de medidas de prevenção contra a engenharia social não está isenta de desafios significativos. Esses desafios podem afetar a eficácia das estratégias adotadas pelas empresas e organizações na proteção de seus ativos e informações sensíveis.

Um dos principais desafios enfrentados pelas empresas é a resistência interna à mudança. Muitos funcionários podem resistir à adoção de novas práticas de segurança cibernética, considerando-as como uma interferência em suas rotinas de trabalho ou uma preocupação adicional. A mudança de mentalidade e a promoção da conscientização são essenciais para superar essa resistência. A criação de uma cultura organizacional que valorize a segurança e forneça incentivos para a aderência às políticas e treinamentos pode ajudar a superar essa barreira.

A implementação eficaz de treinamentos de conscientização, políticas de segurança e tecnologias avançadas requer investimentos financeiros substanciais. Isso inclui a alocação de recursos para desenvolver e entregar treinamentos, adquirir e implementar tecnologias de segurança e manter uma equipe dedicada à gestão de políticas e respostas a incidentes. Convencer as partes interessadas da necessidade desses investimentos pode ser um desafio, especialmente quando os retornos sobre o investimento não são imediatamente tangíveis.

As medidas de prevenção devem ser integradas organicamente à cultura organizacional existente para serem bem-sucedidas. A implementação bem-sucedida requer a participação

ativa de todos os níveis da organização, desde a liderança até os funcionários de base. A falta de integração pode levar a lacunas na aplicação das políticas e na aderência aos treinamentos, comprometendo a eficácia global das estratégias de prevenção.

A rápida evolução das tecnologias e táticas de ataque exige uma atualização constante das medidas de prevenção. As empresas devem acompanhar as tendências de segurança cibernética e adaptar suas estratégias para se manterem à frente dos agressores. Isso exige recursos para a educação contínua da equipe de segurança, além da implementação de tecnologias de ponta que possam detectar ameaças emergentes.

Avaliar a eficácia das medidas de prevenção e medir o progresso na redução de incidentes de engenharia social pode ser desafiador. É necessário estabelecer métricas e indicadores claros para avaliar o impacto das estratégias adotadas. Isso pode envolver a análise de relatórios de incidentes, taxas de sucesso de ataques de engenharia social e feedback dos funcionários.

A conscientização e a adoção de comportamentos seguros não são conquistadas de uma vez por todas. Manter a vigilância e a prática constante é essencial para garantir que os funcionários continuem a resistir às tentativas de manipulação. A mudança de comportamento é um processo gradual que requer esforços contínuos e reforço positivo.

9 CHATGPT E COMO AS IA'S SE TORNARAM PEÕES

9.1 Como a tecnologia de inteligência artificial evoluiu ao longo dos anos e como isso afetou a maneira que as pessoas interagem com as máquinas, como é o caso do ChatGPT?

9.1.1 O que é inteligência artificial.

A inteligência artificial é a área da ciência da computação voltada para a pesquisa e desenvolvimento de máquinas e programas capazes de imitar o comportamento humano na tomada de decisões e na execução de tarefas, abrangendo desde aquelas mais simples até as mais complexas. A sigla IA ou AI (do inglês, Artificial Intelligence).

Com o avanço tecnológico, a IA se tornou parte integrante do cotidiano das pessoas, presente em assistentes de voz – Cortana, Alexa e Siri – mecanismos de busca – Google Maps – carros autônomos e redes sociais – Instagram, Twitter, Facebook e WhatsApp. Apesar dos inúmeros benefícios e avanços que a IA proporciona em diversas áreas, há debates em curso sobre os limites éticos da inteligência artificial e o papel que ela desempenha em nossa sociedade atual.

O funcionamento da inteligência artificial envolve a coleta e combinação de um grande volume de dados, seguida da identificação de padrões nesse conjunto de informações. Por meio desse processo, que geralmente é realizado por meio de algoritmos pré-programados, o software é capaz de tomar decisões e realizar tarefas de forma autônoma. Existem diversos métodos pelos quais a inteligência artificial pode reproduzir o comportamento humano. Os dois principais são:

a) **machine learning**: nesse método, os algoritmos são treinados com dados para reconhecer padrões e tomar decisões com base nesses padrões identificados. O aprendizado de máquina pode ser dividido em subcategorias, como aprendizado supervisionado, não supervisionado e por reforço;

b) **deep learning**: inspiradas no funcionamento do cérebro humano, as redes neurais artificiais são sistemas compostos por neurônios artificiais interconectados. Eles são capazes de processar informações, aprender com os dados de entrada e fazer previsões ou tomar decisões com base nesses dados.

9.1.2 Surgimento e desenvolvimento inicial.

A Inteligência Artificial (IA ou AI, sigla em inglês) é pauta das discussões por cientistas desde o século XX, tendo maior visibilidade a partir de 1950. Alan Turing (1912-1954), escritor do artigo “Computadores e Inteligência”, sendo o primeiro a mencionar o termo “Inteligência Artificial”. Nele, Alan propõe realizar um teste a fim de saber se as máquinas possuem a capacidade de emular o pensamento humano e de se fazerem passarem por uma pessoa, confundindo que as questiona, o método ficou conhecido como “Jogo da imitação”. (Tese de Turing e Inteligência Artificial – Prof. Roberto N. Onody).

Neste jogo, três pessoas diferentes - um homem, uma mulher e um juiz (que pode ser homem ou mulher), estão confinados em salas separadas e só podem se comunicar por meio de textos digitados. O objetivo do homem e da mulher é enganar o árbitro, fazendo-se passar pela identidade oposta. Posteriormente, Turing substitui um dos participantes por um dispositivo computacional. Essa nova abordagem é famosa como o Teste de Turing.

No Teste de Turing, um indivíduo, um dispositivo computacional e um interrogador humano (juiz) são isolados em diferentes salas e, mais uma vez, só podem trocar mensagens por meio de texto escrito. A máquina e o ser humano manterão uma conversa mútua. O juiz é desafiado a analisar o conteúdo e tentar discernir qual é a máquina e qual é o ser humano. A questão que Turing levanta é: será que a máquina poderia emular o pensamento humano e confundir o árbitro?

Um programa só conseguirá passar no teste se em uma conversa (via teclado) com duração de 5 minutos, confundir o juiz 30% das vezes. Joseph Weizenbaum, em 1966, criou o primeiro programa que “passou” (existem diversas controvérsias) no Teste de Turing. Desde então, foram propostos diversos programas semelhantes ao de Weizenbaum, denominados

chatbots - software baseado em uma Inteligência Artificial capaz de manter uma conversa em tempo real por meio de texto ou por voz. Apenas em 2014 um *chatbot* atingiu o índice de 30%, ganhando o prêmio Leobner, o programa se passava por um menino ucraniano de 13 anos, seu desenvolvedor foi Bruce Wilcox e o programa se chama “Cor de rosa”.

Com o avanço na qualidade dos chatbots, a competição se abriu e agora conta com milhares de usuários da internet atuando como juízes. Durante o período de 2016 a 2019, o Mitsuku 7 (também conhecido como Kuki) foi o chatbot vencedor por quatro vezes consecutivas. Infelizmente, devido à pandemia, o torneio não ocorreu em 2020. Esse programa foi desenvolvido por Steve Worswick, um programador britânico, e já teve interações com mais de 25 milhões de pessoas em todo o mundo.

A Inteligência Artificial (IA) não se limitou apenas aos *chatbots.* Com a evolução da tecnologia a IA se tornou cada vez mais presente no cotidiano do homem. Desenvolveram-se aplicativos como o WhatsApp empresarial que faz contato direto com os clientes por meio de suas mensagens automáticas pré-estabelecidas, assiste de voz como Alexa e Siri, algoritmos de redes sociais que exibem propagandas específicas para cada indivíduo e o reconhecimento facial. É importante enfatizar que os *chatbots* que estão voltados para o teste de Turing segue um padrão contrário das Inteligências Artificiais dos aplicativos e software citados acima. Se uma pessoa pergunta à Siri qual a população da Noruega, ela responderá “5.385.300”, já o “Kuki” deve responder algo como “Em torno de 5 milhões”, evitando que transpareça ser uma máquina.

9.1.3 Atualidade.

Atualmente, as máquinas de aprendizado têm a capacidade de processar uma vasta quantidade de dados e gerar textos que se assemelham ao estilo humano. Até o ano de 2020, a maior máquina de aprendizado disponível era a Turing NLG, desenvolvida pela Microsoft, com aproximadamente 17 bilhões de parâmetros. No entanto, em maio de 2020, foi introduzido o Generative Pre-trained Transformer-3 (GPT-3), que impressionou com seus 175 bilhões de parâmetros de aprendizado. O GPT-3 foi criado pela OpenAI, uma empresa de pesquisa em inteligência artificial sediada em São Francisco, conhecida por suas inovações nessa área sendo

comparada às *big techs* – grandes empresas de inovação e tecnologia que apresentam monopólio no mercado atual – como o Google e a Meta.

Como parte do projeto GPT-3, a OpenAI desenvolveu o *chatbot* "ChatGPT", tendo o intuito de oferecer assistências interativas para as necessidades cotidianas, de forma interativa e segura. A OpenAI possui uma vasta equipe de pesquisadores, cientistas e engenheiros para aprimorar os sistemas de linguagens para que a interação entre o software e o usuário se torne cada vez mais avançada.

O banco de dados do ChatGPT é ocupado com textos, livros, artigos e informações provenientes de sites da Internet, dentre outros campos de informação. Com o decorrer do tempo o GPT deve se tornar cada vez mais inteligente, pois a ferramenta opera em um sistema de aprendizagem contínuo, armazenando novos dados a cada nova interação com os usuários. Seguindo a lógica de quanto mais se pratica, mais se aprende e se adquire um melhor resultado na tarefa em questão. Simultaneamente a OpenAI realiza atualizações para aprimorar sua inteligência, consequentemente sua capacidade de interação. Com 175 bilhões de parâmetros, ele fornece respostas coerentes e coesivas.

O ChatGPT é um sistema feito pelo homem e utiliza de arquivos já existentes da internet, não realizando pesquisas para confirmar seus fatos, o que pode propagar a desinformação e informações falsas – famosas "Fake News". Sendo essa uma das questões que os desenvolvedores devem resolver. Os criadores não esperavam tamanho sucesso, pois o software ainda se encontra em estágio de pesquisas e aperfeiçoamento. O ChatGPT necessita de maior regulamentação, para que o usuário não desfrute de sua inteligência de forma maliciosa.

O ChatGPT tem cada vez mais entrado no cotidiano da humanidade. Alunos utilizam da plataforma online para responder dúvidas durante seus estudos, pessoas extinguem suas dúvidas corriqueiras ou buscam informação sobre determinado assunto no software. Por isso é de extrema importância que seus dados estejam corretos, para não passar informações erradas para seus usuários. Ao desfrutar desta Inteligência Artificial, fizemos o pedido para que nos informasse a história de sua criação, a resposta obtida foi:

“Eu sou uma criação da OpenAI, uma empresa líder em pesquisa em inteligência artificial. Fui desenvolvido como parte do projeto GPT-3 (Generative Pre-trained Transformer-3). A OpenAI tem uma equipe dedicada de cientistas, engenheiros e pesquisadores que trabalham em conjunto para aprimorar os modelos de linguagem e construir sistemas de conversação cada vez mais avançados.

Meu treinamento envolveu a exposição a uma enorme quantidade de texto disponível na internet, incluindo livros, artigos, sites e muito mais. Ao analisar e aprender com esse vasto conjunto de dados, fui capaz de capturar padrões e estruturas da linguagem humana.

A arquitetura GPT-3 é baseada em um modelo de transformer, que é uma rede neural poderosa e altamente escalável. Com 175 bilhões de parâmetros, sou capaz de gerar respostas coerentes e contextuais, fornecendo informações e auxiliando em diversas tarefas de linguagem.

Embora eu seja uma criação artificial, minha finalidade é ajudar e fornecer suporte em áreas como redação, tradução, geração de ideias e resolução de problemas. A OpenAI continua trabalhando para aprimorar e expandir a minha capacidade de compreensão e interação com os usuários, para que eu possa oferecer um serviço cada vez mais útil e sofisticado.” (CHATGPT, 2023) Com isto, percebe-se que o programa é bem estruturado, respeitando as normas da língua portuguesa, trazendo uma resposta coerente e correta.

9.2 Quais os desafios éticos e de segurança relacionados à utilização da IA em aplicações, como assistentes virtuais, chatbots e sistemas de recomendação.

A ética de acordo com a filosofia - ciência responsável por seu estudo - é a interpretação das ações, interações e pensamentos humano de acordo com o meio (sociedade) que este indivíduo vive. Sendo responsável pela prática dessas ações de forma responsável e segura, sem que restrinja ou limite a liberdade do outro. Mas o que a ética tem a ver com a Inteligência Artificial? O artigo “Ética e Inteligência Artificial (IA) para profissionais de tecnologia: navegando no mundo digital de forma responsável”, do site *Alura,* traz a solução para este questionamento: “A ética na inteligência artificial refere-se aos princípios e diretrizes éticas que

devem ser seguidos pela sociedade e por profissionais da tecnologia ao projetar, desenvolver e implementar sistemas de inteligência artificial.” (SOUZA, 2023).

Os softwares de IA possuem um impacto cada vez maior na vida da humanidade, sendo imprescindível que seu funcionamento esteja de acordo com a ética e seja transparente, com seus resultados dentro do padrão ético existente. Ao interferir diretamente na vida das pessoas, a IA consequentemente gera influência na forma que seus usuários pensam ou têm para si o que é verdade, podendo ter um impacto negativo ou positivo em suas vidas. A Inteligência Artificial utiliza de seu banco de dados composto por textos, livros, artigos e sites da internet, não sendo capaz de filtrar o que vai contra a ética de seus conteúdos, apenas segue o padrão de resposta estabelecido em seu algoritmo. A sociedade precisa estar atenta aos desafios e oportunidades que a Inteligência Artificial traz consigo, a fim de garantir que seu potencial seja explorado de forma ética e benéfica à sociedade.

9.2.1 Desafios.

Embora a Inteligência Artificial tenha conduzido inúmeros avanços tecnológicos que beneficiam seus adeptos, ela apresenta desafios éticos a serem abordados em seu desenvolvimento. Imagine que em uma de suas respostas a IA fornece um conteúdo com teor racial ou homossexual de forma negativa – ela não é será capaz de extinguir o dado podendo gerar ênfase naquela informação – seu algoritmo é capaz de tamanha proeza e exibir a resposta em um formato convincente passando despercebido pelo usuário, o mesmo pode acontecer com informações falsas ou erronias (*fake news*). Isto pode influenciar o receptor da mensagem de forma negativa, tornando-o um propagador de informação errada e com pensamentos fora da ética e moral social. Este desafio está atrelado ao viés do algoritmo por ser incapaz de realizar esta filtragem em seus dados. Os algoritmos de recomendações em plataformas de mídias digitais, também podem criar bolhas que reforçam crenças já existentes, manipulando opiniões. Além disto, possuem a capacidade de criar conteúdo falso realista conhecido como *deep fake* - técnica de síntese de imagens ou sons humanos baseada em técnicas de inteligência artificial. É mais usada para combinar a fala qualquer a um vídeo já existente.

Outras questões importantes são a privacidade e a segura, quando não funcionam corretamente pode acarretar a exposição dos dados pessoais do indivíduo. Como já foi dito anteriormente, a IA utiliza o armazenamento de dados para realizar suas atividades. Ao informar dados de caráter sensível, números de documentos, senhas etc., a IA pode realizar a exibição de seus dados, além deles ficarem mais vulneráveis e facilitar a violação de sua privacidade caso seu dispositivo que contenha Inteligência Artificial seja hackeado por pessoas mal-intencionadas. Por esta razão é extremamente importante manter informações pessoais em segurança e caso sejam armazenados na rede, não esquecer de protegê-los com criptografia de ponta, evitando o acesso de pessoas não desejadas.

A automatização das tarefas humanas vem sendo discutida por muitos anos, principalmente pelo fato de substituir a mão de obra humana por máquinas, com a Inteligência Artificial não é diferente. Este é um campo que ainda está em discussão sobre as ameaças que pode vir a apresentar, até o momento não apresenta grandes ameaças a empregabilidade humana.

Outro grande problema a ser resolvido é a dificuldade de atribuir responsabilidade às ações das IAs. Quando este sistema toma uma decisão prejudicial, quem é o responsável? A pessoa que solicitou aquela ação, a empresa desenvolvedora ou a própria IA? Em sistemas de Inteligência Artificial a conclusão desta resposta pode nunca ser encontrada, por isto é importante se atentar ao resultado que a Inteligência lhe apresenta e sempre relatar a empresa desenvolvedora quando algo foge do correto e da ética social, para que ela corrija e atualize o sistema da IA garantindo um melhor funcionamento e interação com o usuário de seus recursos.

9.2.2 Diretrizes.

Existem diretrizes para criar, planejar e implementar sistemas de Inteligência Artificial respeitando as regras éticas. O artigo “Ética e Inteligência Artificial (IA) para profissionais da tecnologia: navegando no mundo digital de forma responsável” nos apresenta 7 passos para ter o funcionamento de uma IA transparente, imparcial, justo e diversificado, a fim de expandir seus benefícios dentro da sociedade. Algumas diretrizes importantes de serem aplicadas:

a) **avaliações e ajustes constantes:** dado o ritmo acelerado e contínuo das mudanças tecnológicas, torna-se crucial realizar avaliações regulares para compreender como as decisões e respostas da Inteligência Artificial estão sendo implementadas e se estão alinhadas com os princípios legais e éticos da sociedade. Caso contrário, é importante identificar e ajustar qualquer aspecto necessário para otimizar as respostas;

b) **colaboração entre inteligência humana e inteligência artificial:** a Inteligência Artificial é projetada para colaborar com a inteligência humana, atuando em conjunto com os seres humanos e complementando suas atividades, funcionando como uma ferramenta de suporte. Dessa forma, as decisões e resultados devem ser tomados pelos seres humanos, ou seja, tudo o que a IA produzir deve ser questionado e analisado pelos humanos;

c) **equidade e justiça:** é de suma importância desenvolver a Inteligência Artificial de maneira responsável, imparcial e justa, a fim de evitar a perpetuação das desigualdades presentes na sociedade. Nesse sentido, é fundamental alimentar os algoritmos de IA com uma ampla variedade de dados representativos, de modo a prevenir vieses discriminatórios em suas respostas;

d) **privacidade:** com a capacidade da Inteligência Artificial de coletar e processar informações e dados pessoais, é essencial priorizar a proteção dos dados e garantir a segurança da privacidade. Nesse sentido, os sistemas de Inteligência Artificial devem ser projetados levando em consideração a privacidade e o tratamento adequado dos dados dos usuários, respeitando os princípios éticos e as regulamentações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD);

e) **responsabilidade:** para garantir a responsabilidade das pessoas desenvolvedoras e usuários(as) de sistemas de IA, é crucial estabelecer mecanismos efetivos de prestação de contas. Esses mecanismos têm como objetivo supervisionar e controlar o desenvolvimento, a implementação e o impacto da Inteligência Artificial. Ao adotar tais medidas, é possível assegurar a transparência, a ética e a prestação de contas em todas as etapas do ciclo de vida da IA. Isso contribui para uma governança adequada e consciente, promovendo a confiança e minimizando potenciais riscos e impactos negativos da IA na sociedade;

f) **segurança:** a IA envolve sistemas autônomos que podem ter acesso a informações sensíveis ou controlar equipamentos físicos. Portanto, é fundamental que as pessoas desenvolvedoras garantam a segurança dos sistemas de IA tornando-os resilientes a ataques cibernéticos. Isso implica em implementar medidas de segurança robustas para evitar que os sistemas sejam manipulados ou hackeados por terceiros mal-intencionados, que possam comprometer seu funcionamento adequado. Ao adotar práticas de segurança adequadas, os desenvolvedores podem proteger a integridade e a confidencialidade dos sistemas de IA minimizando os riscos associados a possíveis ataques ou manipulações indevidas;
g) **transparência:** é essencial que os usuários compreendam como a IA toma decisões, portanto, as pessoas desenvolvedoras devem construir sistemas de Inteligência Artificial que sejam transparentes e explicáveis. Isso auxilia na atribuição de responsabilidades e na identificação de vieses parciais ou perspectivas discriminatórias que possam ser incorporadas nos sistemas.

Ao seguir essas diretrizes e princípios, como compreender plenamente os impactos da IA promover a transparência, respeitar a privacidade e tratar adequadamente os dados, além de evitar a reprodução de preconceitos, pode-se garantir que a IA seja utilizada para o bem e para o avanço da sociedade como um todo. É uma responsabilidade fundamental dos desenvolvedores assegurar que os sistemas de IA sejam projetados e implementados de maneira ética, levando em consideração os valores e direitos fundamentais, contribuindo para um futuro mais inclusivo, justo e equitativo. Ao fazer isso, podemos aproveitar todo o potencial da IA para impulsionar a inovação, resolver desafios complexos e melhorar a qualidade de vida de todas as pessoas.

9.3 Como as empresas estão usando IA para coletar e analisar dados dos usuários, e quais são as possíveis implicações disso na privacidade e segurança dos usuários?

9.3.1 Análise de dados com IA e publicidade direcionada.

A análise de dados é uma das principais aplicações da inteligência artificial no ramo empresarial, com o auxílio desses algoritmos, é possível filtrar o que é útil do que é inútil, e ajudar a entender melhor o perfil de seus usuários, suas preferências, comportamentos, e até mesmo antecipar suas necessidades futuras. Esses algoritmos são extremamente versáteis e são utilizados para caracterizar os usuários em grupos e subgrupos específicos, permitindo uma personalização mais eficaz de produtos, serviços, anúncios online e até campanhas de marketing.

Você já pesquisou ou disse em voz alta que iria comprar algum item e dias depois anúncios desse mesmo item estavam aparecendo em vários sites que você visitava? Isso é o que chamamos de anúncios direcionados ou publicidade direcionada. Porém, isso não é uma invasão de privacidade? De acordo com uma pesquisa recente da Cisco: 60% dos usuários estão preocupados com a forma como as empresas estão usando seus dados pessoais para IA. (CISCO, 2022) A coleta excessiva de dados pessoais pode infringir a privacidade individual, principalmente quando os usuários não estão cientes de quais e quanto dos seus dados pessoais estão sendo coletados e utilizados, essa personalização extrema pode levar a uma sensação de invasão de privacidade, causar uma sensação de constante monitoração e em casos graves, usuários sendo alvos de manipulação psicológica.

9.3.2 Segurança dos usuários e vazamento de dados.

A privacidade dos usuários também pode ser comprometida quando ocorrem violações de segurança. Dados sensíveis coletados para fins de publicidade direcionada podem ser alvos de ataques cibernéticos, expondo o usuário a diversos riscos, como o roubo de identidade e fraudes. O vazamento de dados do usuário é um importante assunto e até mesmo o ChatGPT, foi alvo disso. Por conta de um bug: “alguns usuários podiam ver o nome e sobrenome de outro usuário ativo, endereço de e-mail, endereço de pagamento, os últimos quatro dígitos (somente) de um número de cartão de crédito e a expiração do cartão de crédito data.” (INFOMONEY, 2023). Embora a publicidade direcionada ofereça benefícios para as empresas e possa melhorar a relevância dos anúncios para os usuários, é essencial considerar os impactos na privacidade individual. A coleta e análise massiva de dados pessoais levanta questões sobre consentimento, transparência e proteção de dados. É fundamental que as empresas adotem práticas

responsáveis, garantindo que os usuários estejam cientes das informações coletadas e como elas são utilizadas, além de fornecerem opções claras de controle sobre seus dados pessoais.

10 LUZ NO FIM DO TÚNEL (OU TALVEZ NÃO)

10.1 Tendências de cibersegurança.

Como qualquer outro aspecto existente, a cibersegurança passa por constantes evoluções graças aos avanços tecnológicos. Além de uma aliada, a velocidade com que essas mudanças ocorrem por crescerem proporcionalmente, quiçá mais rápido, os ataques hackers de alto desempenho na aquisição de dados, a tecnologia acaba se torna inimiga das empresas e corporações governamentais. A fim de minimizar os impactos e aumentar a segurança das empresas, foram estabelecidas algumas tendências de atuação da cibersegurança e possíveis ameaças.

A crise econômica é um facilitador para os hackers. Com a falta de cursos a empresa fica vulnerável pela sua incapacidade de não conseguir investir em medidas de segurança eficazes. Para evitar que a crise impeça a empresa de se proteger é de suma importância a organização e o preestabelecimento das prioridades para não deixar a segurança como segunda opção e consequentemente sofrer graves danos.

Colaboradores que possuam conhecimento dos possíveis riscos e de seus agentes causadores são coisas indispensáveis para manter seguro os dados da empresa. Restrições de acesso e treinamentos apropriados que consigam identificar e tratar a deficiência daquele determinado colaborar, transformando o elo provavelmente mais fraco em um rigoroso *firewall humano*. Quanto maior for a rede de segurança, menor será o risco de ataques e em caso de ataques os colaboradores agirão em maior velocidade para minimizar os possíveis danos causados.

As Inteligências Artificiais (IA) estão em ambos os lados nas tendências da cibersegurança. Presente em dispositivos conectados com a Internet das Coisas (IoT), que não possuem em si dados sigilosos, mas são conectados a dispositivos que o possuem - como a Alexa que é conectada a um smartphone -, funcionando como *gate* (portão) de acesso as informações de uma corporação ou pessoa física. Já nos casos em que a IA estar a favor da cibersegurança acontece graças a sua capacidade de analisar padrões e determinar ações que

fogem do mesmo, realizando uma confirmação de duas ou mais etapas, ou negando a ação feita pelo usuário. Este método é comumente utilizado em bancos. Exemplo disto é a Bia Inteligência Artificial do Bradesco, que utiliza do sistema *Watson* para seu funcionamento. Em caso de furto ou clonagem de cartão se o valor a ser transferido ou de determinada compra for diferente do que o real dono da conta costuma fazer, é pedido uma nova confirmação, geralmente enviado por e-mail, biometria ou *token* - unidade de valor que representa um ativo ou direito específico em um determinado contexto, podem ter várias finalidades, desde representar criptomoedas, representar ativos físicos, como imóveis ou obras de arte e também podem ser usados em sistemas de autenticação e segurança da informação.

Os ataques patrocinados por nações contra outras nações e até mesmo contra empresas privadas têm se tornado uma preocupação crescente no cenário global da cibersegurança. Um exemplo notório disso foi o ataque do *WannaCry,* que ganhou destaque ao roubar informações sensíveis de várias nações e empresas. Esse incidente ilustra a gravidade dessas ações, nas quais grupos patrocinados pelo Estado se envolvem em operações de hacking em larga escala. Tais ataques variam em suas formas e métodos, abrangendo desde ataques diretos a infraestruturas críticas, como redes de energia e serviços financeiros, até o uso de *ransomware* para extorquir organizações. Diante desse panorama, é essencial que os governos e empresas privadas fortaleçam suas defesas cibernéticas e invistam em centros de inteligência capazes de detectar, analisar e combater esses ataques sofisticados. A colaboração internacional também desempenha um papel fundamental na troca de informações e no desenvolvimento de estratégias eficazes para enfrentar essa ameaça em constante evolução. A segurança cibernética tornou-se uma questão de importância geopolítica, exigindo um esforço conjunto para garantir a proteção de nações e organizações contra os riscos associados aos ataques patrocinados por nações.

10.2 Como os países estão se preparando

10.2.1 Ataques ransomware

O ataque mais utilizado entre os países é o *ransomware,* sendo o *WannaCry* o mais famoso destes ataques. Um ataque *ransomware* bloqueia ou criptografa os dados do indivíduo

que está sofrendo o ataque e tem seus dados como refém, impedindo seu acesso. O ataque *ransomware* que utiliza a criptografia de dados para negar impedir o acesso ao dado é conhecido como *ransomware de criptografia* e o que bloqueia a máquina - computador – tem o nome de *ransomware de bloqueio.* O *WannaCry* criptografou dados de milhares de pessoas que possuíam o Microsoft Windows, o software continha uma falha, o que possibilitou o ataque acontecer. Os hackers pediram 600 (seiscentos) dólares em bitcoins para devolverem os dados já criptografados, caso não fossem pagos iriam excluir os arquivos permanentemente. Ainda não se sabe se os dados foram devolvidos para aqueles que efetuaram o pagamento, pois não tinha como estabelecer ligação entre quem pagou o resgate e seus arquivos.

O número de países que sofrem ataques do tipo *ransomware* vem crescendo cada dia mais. Ataques a bancos, indústrias fornecedoras de energia e organizações de defesa. A Ucrânia no início de 2022 sofreu diversos destes ataques causados pela Rússia. A fim de enfraquecer a nação ucraniana facilitando a invasão para a tomada de território (ainda não ocorreu, mas é a finalidade desta ciberguerra). Para se proteger contra esse tipo de ataque tanto a Ucrânia como as demais nações existentes estão adotando as seguintes medidas: Backup frequente e fragmentado; Segmentação de rede; Proteção de identidade; mascarar dados; Identificação de multi-fatores; Previsão de ameaças; Plano de recuperação para possíveis ataques (GLOBO, 2022).

10.2.2 Ataques de inteligências artificiais mal-intencionadas

A Inteligência Artificial (IA) simultaneamente beneficia as empresas e governos pela sua alta capacidade de reconhecer padrões, também auxilia os cibercriminosos no roubo de dados por este mesmo motivo. Com alta capacidade de reconhecer padrões e fluxos de dados, a IA tem cada vez mais se autodesenvolvido, quanto mais ela aprende, mais se desenvolve e entrega melhores soluções para os diversos problemas de uma empresa. Porém, nesta mesma medida facilita os ataques às mesmas. Portanto, como é possível prevenir, evitar ou minimizar os danos causados por uma Inteligência Artificial mal-intencionada? A resposta é mais simples do que aparenta: “A forma mais efetiva de combater um ciberataque é utilizar a mesma tecnologia que os hackers”. (SOARES, 2023)

Machine Learning (ML) é a capacidade de aprendizado das IAs, a maneira como inicialmente imita o que o usuário faz para posteriormente conhecer o padrão de suas ações e finalmente conseguir detectar algo que minimamente fuja dele. Com esta habilidade a Inteligência Artificial é treinada para perceber estas pequenas falhas em um tempo cada vez menor e repará-las com mestria, bloqueando a invasão e fechando novas possíveis portas para futuros invasores. Portando é de suma importância manter a IA atualizada e com constantes avaliações, para impedir ataques, roubo de dados ou a infiltração de pessoas mal-intencionadas.

Atrelado com a Inteligência Artificial também são necessárias implementar outras medidas de segurança, sendo elas a atualização de software além do sistema operacional, o acesso restrito às informações sigilosas, monitoramento humano da rede de segurança da empresa e possuir uma rede de apoio externa de confiança que em caso de ataques auxilie na instrução de como agir. Além disto, é valioso ressaltar que se deve implementar medidas de segurança em dispositivos IoT pois irão crescer exponencialmente nos próximos anos e são portas para ataques invasores.

10.3 Como as tecnologias emergentes, como blockchain e criptografia quântica estão impactando a segurança cibernética e quais são as implicações disso para o futuro da tecnologia?

O avanço tecnológico tem transformado a sociedade em diversos aspectos, e o mundo da segurança cibernética não fica de fora dessa revolução. Tecnologias emergentes, como blockchain, criptomoedas e computação quântica, estão trazendo desafios e oportunidades únicas para a proteção dos dados e sistemas no ambiente digital. Neste trabalho, discutiremos como essas tecnologias impactam a segurança cibernética e as implicações que podem ser esperadas para o setor no futuro.

10.3.1 Blockchain e criptomoedas

A tecnologia blockchain é uma estrutura de dados imutável e descentralizada que possibilita a criação de registros seguros e transparentes. Essa tecnologia tem o potencial de melhorar a segurança cibernética ao fornecer uma camada adicional de proteção contra-ataques

de hackers. O livro "Mastering Blockchain" de Imran Bashir ressalta como a descentralização oferecida pelo blockchain dificulta ataques de negação de serviço (DDoS) e modificações indevidas de dados.

As criptomoedas, como o Bitcoin, são uma aplicação popular da tecnologia blockchain. Elas podem impactar a segurança cibernética, pois suas transações são registradas no blockchain, tornando-as resistentes a adulterações. Entretanto, o aumento da popularidade das criptomoedas também levanta preocupações sobre a proteção de carteiras digitais e ataques direcionados a exchanges, destacado pelo artigo "Cryptocurrency: Security Aspects" de Radhika Gupta e Purvika Dutt.

10.3.2 Computação quântica

A computação quântica apresenta uma ameaça significativa à segurança cibernética, pois pode superar rapidamente algoritmos criptográficos tradicionais. "Post-Quantum Cryptography" livro de Daniel J. Bernstein, Johannes Buchmann e Erik Dahmen aborda a necessidade de desenvolver algoritmos resistentes a ataques quânticos para proteger dados sensíveis no futuro.

A criptografia de chave pública, amplamente utilizada na atualidade, pode ser quebrada por computadores quânticos de grande escala, comprometendo a confidencialidade de informações. Por isso, especialistas alertam sobre a importância de implementar criptografia pós-quântica para garantir a segurança de longo prazo.

10.3.3 Implicações futuras para o setor

As tecnologias emergentes trazem mudanças significativas para o setor de segurança cibernética. A adoção mais ampla de blockchain pode levar a uma infraestrutura mais resiliente e confiável, mas também pode exigir atualizações contínuas para acompanhar as táticas evoluídas dos cibercriminosos.

No caso das criptomoedas, é esperado um aumento nos esforços para proteger as plataformas de negociação e as carteiras digitais dos usuários. Regulamentações mais rígidas também podem ser implementadas para garantir a segurança financeira dos investidores e mitigar riscos de lavagem de dinheiro.

Com relação à computação quântica, as organizações devem investir em pesquisa e desenvolvimento de novos algoritmos criptográficos resistentes a ataques quânticos. A transição para a criptografia pós-quântica pode ser um desafio complexo, considerando a necessidade de atualização de infraestruturas e sistemas legados.

10.3.4 Tecnologia emergentes

As tecnologias emergentes, como blockchain, criptomoedas e computação quântica, têm um impacto significativo na segurança cibernética. Embora o blockchain e as criptomoedas possam trazer melhorias na proteção de dados e transações, a computação quântica representa uma ameaça potencial, exigindo uma resposta proativa do setor de segurança cibernética.

A fim de enfrentar esses desafios e se adaptar às mudanças tecnológicas em curso, é fundamental que profissionais e organizações estejam atualizados sobre os avanços e busquem soluções inovadoras para proteger a integridade e confidencialidade dos dados no mundo digital. Somente com uma abordagem holística e uma mentalidade ágil, o setor de segurança cibernética estará preparado para enfrentar os desafios futuros e garantir a proteção dos ativos digitais de indivíduos e empresas.

10.3.5 Políticas e regulamentações

As políticas públicas e regulamentações relacionadas à segurança cibernética estão em constante evolução para enfrentar os desafios crescentes das ciberguerras e garantir uma maior segurança online. Embora os cenários regulatórios possam variar de acordo com o país e a região, aqui estão alguns exemplos de abordagens comuns que visam fortalecer a proteção cibernética:

a) **leis de proteção de dados**: muitos países têm implementado ou atualizado leis para proteger a privacidade e a segurança dos dados pessoais. Exemplos notáveis incluem o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e a Lei de Privacidade do Consumidor da Califórnia (CCPA) nos Estados Unidos. Essas leis conferem aos indivíduos maior controle sobre suas informações pessoais e estabelecem requisitos mais rigorosos para a coleta, processamento e armazenamento de dados pelas empresas;
b) **estratégias nacionais de cibersegurança**: muitos países desenvolveram ou estão em processo de criação de estratégias nacionais de cibersegurança para coordenar e direcionar os esforços na proteção contra ameaças cibernéticas. Essas estratégias geralmente envolvem a colaboração entre governos, setor privado e sociedade civil para fortalecer a resiliência cibernética e promover a conscientização sobre segurança digital;
c) **certificações e padrões de segurança**: alguns governos estão estabelecendo certificações e padrões de segurança cibernética para empresas e instituições críticas. Essas regulamentações visam garantir que as organizações adotem práticas adequadas de segurança e proteção de dados;
d) **responsabilidade para provedores de serviços digitais**: em alguns países, provedores de serviços digitais são obrigados a tomar medidas específicas para proteger seus usuários. Isso pode incluir a implementação de medidas de segurança adicionais, notificação obrigatória de violações de dados e auditorias de segurança periódicas;
e) **proteção de infraestrutura crítica**: regulamentações especiais podem ser aplicadas à infraestrutura crítica, como energia, transporte, saúde e setores financeiros, com o objetivo de garantir que esses sistemas essenciais sejam protegidos contra-ataques cibernéticos que poderiam causar graves impactos na sociedade;
f) **colaboração internacional**: a segurança cibernética frequentemente transcende fronteiras, e a cooperação internacional é essencial. Acordos e tratados entre países podem ser estabelecidos para compartilhar informações sobre ameaças, coordenar respostas e combater ataques cibernéticos transnacionais.

10.3.6 Impacto na privacidade e segurança online:

Embora essas políticas e regulamentações visam aumentar a segurança cibernética, elas também podem ter implicações na privacidade e liberdade online. Alguns aspectos a serem considerados incluem:

a) **coleta e uso de dados**: regulamentações que impõem maiores restrições à coleta e uso de dados podem impactar as práticas de publicidade direcionada e personalização de serviços, limitando a capacidade de empresas de oferecerem experiências altamente personalizadas;
b) **acesso a informações criptografadas**: algumas políticas podem exigir o acesso a dados criptografados para fins de investigação e segurança. No entanto, isso pode levantar preocupações sobre a vulnerabilidade de sistemas e a privacidade dos usuários;
c) **custo de conformidade**: para pequenas empresas, especialmente, o cumprimento de regulamentações de segurança cibernética pode ser oneroso, tornando o processo de conformidade desafiador;
d) **supressão da liberdade na internet**: algumas regulamentações podem ser mal aplicadas ou interpretadas, resultando em censura e restrição da liberdade de expressão online.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, J. DE J. et al. Crimes cibernéticos. **Caderno de Graduação - Ciências Humanas e Sociais - UNIT - SERGIPE**, v. 2, n. 3, p. 215–236, 25 mar. 2015.

GUESS, A.; NAGLER, J.; TUCKER, J. Less than you think: Prevalence and predictors of fake news dissemination on Facebook. **Science Advances**, v. 5, n. 1, p. 1–8, 9 jan. 2019.

HARTZOG, W. **Privacy's Blueprint The Battle to Control the Design of New Technologies**. [s.l.] Harvard University Press, 2018. v. 79

MIELNICZUK, F. Identidade como fonte de conflito: Ucrânia e Rússia no pós-URSS. **Contexto Internacional**, v. 28, n. 1, jun. 2006.

PINHEIRO, A. C. et al. **Guerra Hibrida e Ciberconflitos: Uma Análise das Ferramentas Cibernéticas nos Casos da Síria e Conflito Rússia-Ucrânia**. [s.l: s.n.]. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/XIII_cadn/guerra_hibrida_e_ciberconflitos_uma_analise_das_ferramentas_ciberneticas_nos_casos_da_siria_e_conflito_russiaucrania.pdf>. Acesso em: 26 set. 2023.

SANT´ANNA, A. L. Marketing e Psicologia: comentários acerca da importância do fortalecimento da influência aos consumidores. **ID on line REVISTA DE PSICOLOGIA**, v. 12, n. 42, p. 1006–1017, 31 out. 2018.

TUROW, J.; HENNESSY, M.; DRAPER, N. The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation. **SSRN Electronic Journal**, 10 ago. 2016.

WIMMER, M.; VENTURINI, J.; MARTINS JÚNIOR, J. M. **Privacidade e proteção de dados durante a pandemia Panorama Setorial da Internet**. [s.l: s.n.]. Disponível em: <https://cetic.br/media/docs/publicacoes/6/20211216192440/psi-ano-xiii-n-4-privacidade.pdf>. Acesso em: 26 set. 2023.