RISCO DA CIBERSEGURANÇA NA SITUAÇÃO PANDÊMICA DO COVID-19

Renan Viecili Lameu[1],
Kevyn Phillipe Gusmão,[2]
Elionai de Souza Magalhães,[2]
Bruno Bastos Stoll[2]

[1] Discente do curso de Engenharia da Computação do Centro Universitário Multivix Vitória
[2] Docentes do Centro Universitário Multivix Vitória

RESUMO
O presente trabalho de conclusão de curso tem por finalidade transcorrer a relação dos incidentes de ataques cibernéticos que cresceram devido a situação pandêmica do COVID-19. Esta situação levou instituições, bancos, empresas e escolas a adotarem medidas preventivas para não disseminar o vírus. A forma de combater foi aderir ao distanciamento social, muitas organizações no sentido de não parar o funcionamento, a escolha foi levar funcionários e alunos a continuar suas tarefas para o trabalho remoto. A privacidade e segurança foram fatores nos quais não causaram preocupações para as organizações. Em visão disso, as pessoas utilizando diversos dispositivos sem a proteção recomendada, suas casas se tornaram oportunidades para serem alvos de invasores. O artigo apresenta a definição do termo cibersegurança; os principais ataques que receberam destaque na pandemia em *home-office*, conceitos e aplicação da lei geral proteção de dados nas empresas; dados coletados de reportagem de impactos do COVID-19 no ciberespaço; medidas preventivas e enfim finalizando com o resultado do artigo bibliográfico.
PALAVRAS-CHAVE
Ataques Cibernéticos; COVID-19; Trabalho Remoto; Segurança; Ciberespaço.

ABSTRACT
The purpose of this final paper is to present the list of cyber-attacks incidents that have grown due to the COVID-19 pandemic situation. This situation has led institutions, banks, companies, and schools to adopt preventive measures to avoid spreading the virus. The way to fight was to adhere to social distancing, many organizations in the sense of not stopping the operation, the choice was to take employees and students to continue their tasks for remote work. Privacy and security were factors that did not cause concerns for organizations. In view of this, people using various devices without the recommended protection, their homes became opportunities to be targets of intruders. The article presents the definition of the term cybersecurity; the main attacks that were highlighted in the home-office pandemic, the concept and application of general data protection laws in companies; data collected from reporting on the impacts of the COVID-19 in cyberspace; preventive measures and finally ending with the result of the bibliographic article.
KEYWORDS
Cyber Attacks; COVID-19; Remote-work; Security; Cyberspace.

INTRODUÇÃO

No contexto de modelo de globalização desencadeou a evolução da tecnologia proporcionando fatores para o surgimento da internet, onde foi o marco inicial do seu próprio uso: gerar comunicações entre as pessoas, acesso a plataformas de *streaming*, como Netflix, Spotify, Youtube e entre outros. Onde se encontra uso de

dados, a nova era digital vem crescendo em massa devido a cada usuário exportar conteúdos (fotos, vídeos, texto e músicas) nas nuvens.

Devido a pandemia do COVID-19 o uso de dispositivos eletrônicos conectados à internet se intensificou, facilitando abordagens de hackers na execução de ataques. Dessa forma, pesquisas recentes apontam que houve crescimento de crimes cibernéticos. O modelo adotado para a população de *home-office* favorece os cibercriminosos, pois expõem vulnerabilidades em computadores pessoais. Sendo que a maior parte não apresenta segurança nos dispositivos conectados à própria rede local. Esse aumento de crimes cibernéticos durante a pandemia trata-se de um grande perigo para empresas no ramo da saúde, econômico e na educação. A população tem que ficar em alerta, pois todos estão vulneráveis a sofrer qualquer tipo de ataque virtual. O recorrente artigo bibliográfico identifica padrões de incidentes relacionados aos ataques cibernéticos no período pandêmico e aponta a importância da política de segurança de dados, com base em texto, imagens e informações retirados de jornais, estudos e fontes confiáveis.

1. DEFINIÇÃO DO PROBLEMA

Por qual motivo a pandemia afetou o ciberespaço devido à onda de ataques causados por cibercriminosos que aproveitam as vulnerabilidades do trabalho remoto de empresas e nos setores da saúde.

1.1 Justificativa do Tema

A presente pesquisa se justifica com relação ao atual cenário pandêmico onde a situação fez com que as rotinas de todos mudasse de uma hora para outra. E consequentemente o distanciamento social desencadeou o aumento do uso de dispositivos eletrônicos. Além disso, organizações liberaram sistemas de filiais próprias para funcionários e alunos manterem suas tarefas com uso de aparelhos pessoais desprotegidos. Essas situações chamaram a atenção de cibercriminosos. Nesse sentido, a proposta é trazer reflexão dos motivos de ataques cibernéticos, introduzir breve conhecimento de cibersegurança e medidas preventivas que possam ser adotadas.

1.2 Delimitação do Tema

Abordagem do conteúdo de cibersegurança e os principais tipos de ataques, políticas de segurança e a situação da pandemia no mundo digital, destacando formas de manter dispositivos pessoais protegidos.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Analisar o conhecimento de sistema da informação e segurança de dados, com o novo modo de realidade está sendo inserido no distanciamento social encontrado mundialmente, atribuindo a fatores de indivíduos mal-intencionados que cometem tipos de ataques que os beneficiam e empregam práticas ilegais em dispositivos pessoais.

1.3.2 Objetivos Específicos

A) Apresentar a importância da área de Cibersegurança, identificando como o setor está presente no cotidiano da sociedade;

B) Revisar os impactos da pandemia do COVID-19, relacionados os termos abrangentes de Sistema da Informação e ataques cibernéticos;

C) Introduzir métodos práticos e teóricos em relação a segurança de informação com base a política de dados;

D) Demonstrar formas eficazes para proteger dispositivos pessoais prevenindo ser alvo de hackers.

2. METODOLOGIA

2.1 Tipo de Pesquisa

De acordo com a taxonomia introduzida por Vergara (2000, p.46), a pesquisa teve apoio dos seguintes tipos de pesquisas: Pesquisa Bibliográfica: Análise de material necessário para o entendimento do assunto relacionado às palavras; Pesquisa Documental: Utilização de material publicado sobre o assunto de segurança, tipos de ataques e medidas de proteção.

2.2 Coleta de Dados

Para o presente trabalho realizou-se uma pesquisa bibliográfica. Para DEMO (2000, p.20) pesquisa é entendida como ferramenta de fabricação e aprendizagem com fins científico e educativo, sendo parte do processo para o conhecimento e "somar" no campo de relação do conteúdo. Como afirma Severino (2007), trata-se de registros disponíveis cujo decorre pesquisas comprovadas, documentadas em teses, artigos, textos e jornais, assim os textos se transformam em fontes de temas para serem utilizados na pesquisa. A finalidade da pesquisa é resolver problemas e solucionar dúvidas a partir de procedimentos com base em coleta de formações onde seja para investigar o problema.

Realizou-se uma busca a partir de publicações via google acadêmico de origem internacional e conteúdo relacionado ao tema de segurança da informação e cibersegurança de origem nacional. A seleção realizada entre 14 artigos, resultou a busca do conteúdo a partir de palavras-chave:

"Cybersecurity"," COVID-19"," Pandemic"," Threats"

3. FUNDAMENTAÇÃO TEÓRICA

3.1 Cibersegurança

Cibersegurança (cybersecurity) se baseia no termo referente, proteção e garantia de dados, principalmente aquela ligada a infraestruturas críticas a redes de comunicações e sistemas de informações.

Com base Melo (2017, p.21) é muito comum os profissionais da área serem capazes de testar práticas para adquirir novas metodologias de defesa a sistema, assim profissionais adquirem conhecimento para estudos futuros.

É importante ressaltar que todo tipo de ataque virtual possui um alvo específico que tende a explorar uma falha ou vulnerabilidade de um sistema a ponto de o invasor aproveitar da situação em aqueles que são leigos aos conhecimentos no setor da segurança cibernética. Muitas das vezes é determinado, cujo responsável pela ação do ataque é nomeado de "autor".

Para a definição de escolha de artigos, optou-se pelos artigos publicados nos anos de 2019 a 2021. Após a leitura dos artigos escolhidos foram selecionados os específicos para criação da bibliografia. A seguir será introduzido no Quadro I, a

identificação sequencial dos artigos de busca onde a organização da tabela de forma da qual a ordem de acesso.

Quadro 1 – Lista de artigos selecionados via google acadêmico

Ano	Título do artigo	Autor	Periódico
2016	Cybersecurity in healthcare: A systematic review of modern threats and trends	Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson D. Kyle Monticone	Technology and Health Care 25 (2017) 1–10
2020	Cybercrime Pandemic	Marites V. Fontanilla	Journal of Asian and International Bioethics 30, pag. 161-165
2020	WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19	Debra J. Borkovich, Robert J. Skovira	Issues in Information Systems Volume 21, Issue 4, pag. 234-246
2020	Cybersecurity Risks in a Pandemic	Christina Meilee Williams, Rahul Chaturvedi, Krishnan Chakravarthy	JMIR Publications Vol 23, Vol 22, N° 9
2020	Data Security and privacy in times pandemic	Luis Fernandes	Digital Privacy and Security Conference 2021
2021	CIBERSEGU RANÇA E CIBERDEFESA EM TEMPOS DE PANDEMIA	Helena Carreiras, André Barrinha, António Gameiro Marques, Lino Santos, Daniela Santos, Helder Fialho de Jesus, João Barbas, João Confraria, Luis Borges Gouveia, Paulo Fernando Viegas Nunes, Sofia José Santos and Sofia Martins Geraldes	IDN brief
2020	COVID-19 Pandemic cybersecurity issues	Bernardi Pranggono, Abdullahi Arabo	Internet Technology Letters, Volume 4, Issue 2
2021	Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review.	He Y, Aliyu A, Evans M, Luo C	JMIR Publications Vol 23, N° 4 (2021)

Fonte: Dados da pesquisa

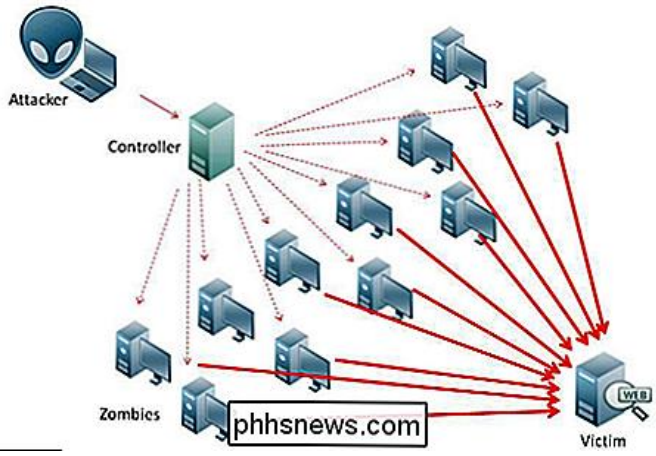
3.2 Tipos de Ataques

Em geral, todo sistema deve conter uma segurança para evitar problemas de vulnerabilidades. As vulnerabilidades são resultado de ameaças, para Dantas (2011). As ameaças estão divididas em: **ameaça natural** designada pelos fenômenos da natureza (terremotos, tempestade, tsunamis, vulcões etc.). **Ameaça involuntária** são resultado de fatores não intencionais, porém, geram dano. Como exemplo, erros, acidentes e aquele que é voltado para o setor de tecnologia é um vírus anexado na caixa de entrada. Uma **ameaça intencional** é aquela que possui objetivo de causar um dano, como invasões, sabotagem, espionagem, fraudes e roubo de informação. É importante entender os principais problemas no ciberespaço.

Knight (2014, p. 99) relata que os principais problemas no mundo cibernético são: “Invasões de privacidade, terrorismo, *phishing*, espionagem política e econômica, tráfico de drogas, pirataria, abuso infantil, spam são as principais ameaças da guerra cibernética”. Desse modo, segue abaixo métodos às ameaças utilizadas mais frequente por cibercriminosos:

- **DoS (Negação de serviço)** – tipo de ataque onde o autor da ação sobrecarrega um servidor ou uma rede com o interrompimento temporário a partir de vulnerabilidades de um protocolo ou serviço. Ocasiona a base de informações negadas, o sistema fora do ar e envio de muitos pacotes de requisições, assim causando o sobrecarregamento do dispositivo (CONKLIN, 2018).

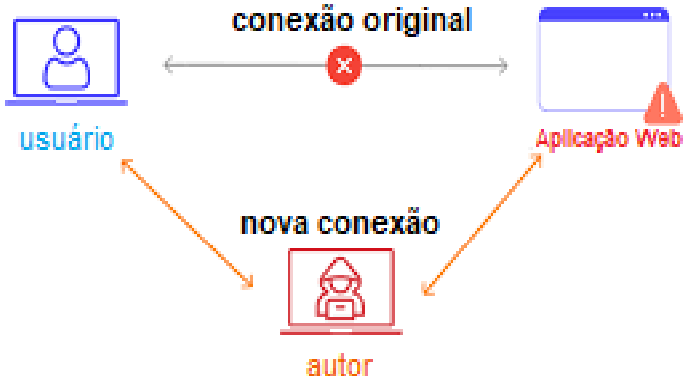
Figura 1 – Ataque de negação de serviço



Fonte: Disponível em https://pt.phhsnews.com/what-are-denial-of-service-and-ddos-attacks3141

- **Man-in-the-Middle**– ataque que intercepta a comunicação numa linha de tráfego entre usuário e o servidor ou usuário e usuário. O elemento observa a rota de pacotes a ponto de modificar, bloquear ou mudar o tráfego da informação (CONKLIN, 2018).

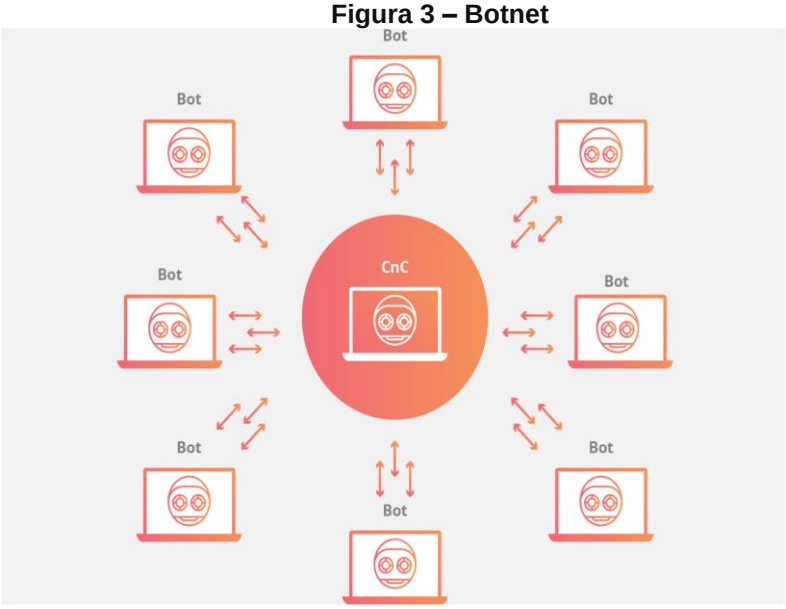
Figura 2 – Ataque Man-in-the-middle



Fonte: Disponível em https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attack

- **Botnet**– envolve em diversos dispositivos eletrônicos onde foram infectados por um malware que está sendo controlado pelo autor. O termo Botnet é designado “rede robô” é composta por milhares dispositivos conectados para roubar dados de usuários, invadir domínios e executar ataque DoS dinâmico (MEYERS, 2021).

Figura 3 – Botnet



Fonte: Disponível em https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-botnet/

- **Phishing** – tipo de ação que, o autor utiliza engenharia social, envia um e-mail malicioso contendo um link, parece confiável as informações do alvo escolhido pelos interceptores da ação, funciona de tal modo quando indivíduo click no link, ele é redirecionado a um website falso assim, roubando dados pessoais ou um malware pode ser instalado no dispositivo (REISSWITZ, 2012).

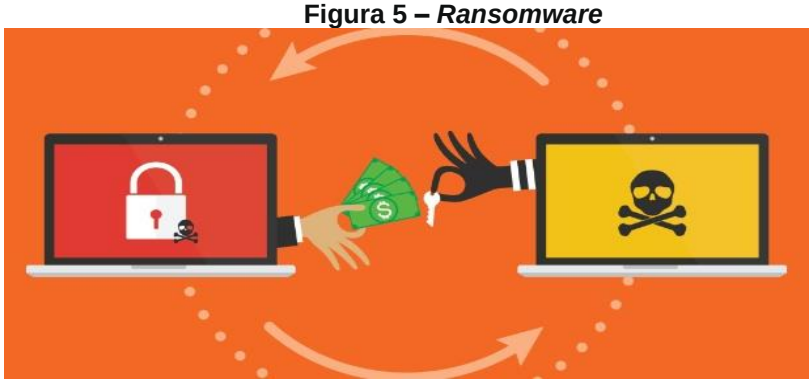
Figura 4 – Ataque Phishing

Fonte: Disponível em https://blog.neoway.com.br/phishing/

- **Engenharia Social** – prática usada para persuadir o indivíduo para conseguir acesso a informações pessoais após uma breve pesquisa do alvo (FRAGA,2019).

- **Ransomware** – Para (CONKLIN, 2018), trata-se de ataques onde o autor bloqueia acesso do sistema do usuário pedindo o pagamento em troca da liberação. Geralmente o pagamento solicitado é em bitcoins (moeda virtual) e caso o autor não receba a quantia pedida todas as informações do sistema são deletadas.

Figura 5 – *Ransomware*

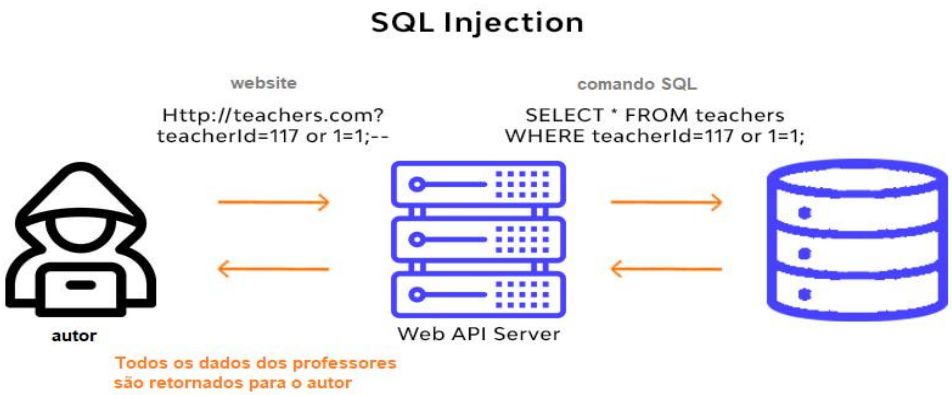


Fonte: Disponível em https://www.uol.com.br/tilt/noticias/redacao/2018/06/16/ransomware-por-que-este-e-o-ataque-virtual-da-moda.htm

- **Brute force** – Ataque do tipo que envolve adivinha combinação de senha em diversas tentativas (BALOCH,2015). Nos dias atuais existem sistemas que possuem um limite de tentativa de senha, assim impedindo o comportamento do ataque.

- **SQL Injection**– tipos de ataques usados em banco de dados com objetivo de controlar e roubar dados, o autor aproveita uma vulnerabilidade do código interno para aplicar instrução de comandos maliciosos no SQL (FRAGA,2019).

Figura 5 – SQL *Injection*



Fonte: Disponível em https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1

3.3 Políticas de Segurança da Informação

A política de segurança sempre está recebendo atualizações, pois para Geus e Nakamura (2007, p.25), no ciberespaço “é caracterizado por meio de uma evolução contínua onde a cada novos ataques abrangem as novos métodos de proteção que levam ao desenvolvimento de técnicas de ataques mais eficientes e formam um ciclo”. Geus e Nakamura (2007) faz sugestões para evitar riscos é focar em pontos: entender o modo de ataque; prestar atenção nas novas tecnologias pois há possíveis falhas; sempre haverá novas maneiras de ataques conforme a evolução da tecnologia.

O conceito da segurança da informação, para Fernandes (2014, p.326), está relacionado à proteção de informações de determinadas pessoas ou companhias. Uma informação é denominada como qualquer tipo de dado de valor, podendo ser público ou privado. Atribuem ferramentas para obtenção a níveis de proteção, porém as informações têm a possibilidade de serem afetadas por fatores internos: um terceiro pode fazer a alteração, destruir ou criptografar dados. Com base o que foi discutido possui três princípios responsável pela política de segurança: **Confidencialidade**: propriedade cujo permite apenas pessoas autorizadas pelo legítimo proprietário a ter o acesso às informações; **Integridade**: propriedade cujo mantém as informações a suas características atribuída ao proprietário da informação; **Disponibilidade**: propriedade cujo permite a informações esteja liberada apenas para quem possui a autorização.

3.4 Direitos da LGPD Fornecida para Usuários

O Brasil é o primeiro país a promulgar uma lei de proteção de dados na constituição de 1988 e após 22 anos foi implementada uma lei geral de proteção de dados (LGPD) abrangendo o espaço cibernético onde seria validada em 2020. Foi o marco no ambiente tecnológico nacional a receber os devidos tratamentos que circulam pelo ciberespaço (MALDONADO, 2019).

Com base no contexto histórico, a LGPD é uma lei do departamento federal no qual emite a proteção nacional e tratamentos de dados pessoais em mercados e setores. A lei prevê a proteção da privacidade e da liberdade pessoal, a norma foi adotada nas preocupações em ambientes financeiros, empresariais e tecnológicos para limitar de invasores e souber lidar com informações mediante a estruturas flexíveis em ramo de grande porte.

Em vigor do congresso nacional, a lei nº 13.853 de 2018 nomeada lei geral de proteção de dados pessoais (LGPD), Diante do que foi relatado o artigo 46 é responsável por sigilos de dados e nele é dialogado com o seguinte:

> Artigo 46. A pessoa deve tomar medidas de segurança e medidas para manter a proteção dos dados pessoais de acesso não permitido, acesso ilegal ou danos e alteração de informação.
>
> §1º As autoridades nacionais possuem o poder de exercer o tipo de informação tratada a níveis técnicos vigente e formular normas técnicas para aplicação da norma proposta, em ocasiões especiais os dados mantém cautelas de acordo com o art. 6º (o indivíduo tem que 'informar as autoridades de maneira imediata devido eliminação, bloqueio ou uso de compartilhamento de dados).

Vigente de sofrer alguma ameaça cibernética, o titular deve fazer o boletim de ocorrência seguindo as regras dadas ao artigo 48, descrito abaixo:

> Artigo 48. O indivíduo deverá comunicar às autoridades a ocorrência de incidente no qual infringem as leis de LGPD.
>
> §1º O prazo de comunicação deverá ser feito em adequado ao acontecimento e deverá ser mencionado:
>
> I – Descrição dos dados pessoais prejudicados;
>
> II – Informações sobre os envolvidos;
>
> III- Risco envolvidos ao acontecimento;
>
> IV- Caso a comunicação às autoridades não for ocorrida de forma imediata, a vítima deve justificar;
>
> §2º O caso de gravidade do incidente vai ser avaliado por autoridades nacionais:
>
> I – Divulgação do incidente a partir de meios de comunicações;
>
> II – Adoção de medidas preventivas ou reversão do ocorrido.
>
> §3º Avaliação eventual do ocorrido com comprovações que medidas foram aplicadas para obter os dados pessoais afetados a tornar não autorizados para terceiros.

4. CIBERATAQUES DURANTE A PANDEMIA

Com base no relatório do Julius Baer, banco suíço (MOURA; HAIDAR, 2020), a expectativas de custos causada por ameaças cibernéticas global em torno de US $6 trilhões em 2021, conforme na Figura 6. Apesar do caos do coronavírus para a população deve entrar em alerta ao índice de expansão de golpes sendo aplicados em relação ao tema COVID-19, onde *hackers* exploram o alvo enviando malware e aplicação de *phishing.* De acordo com o levantamento do Google, na semana de abril, mais de 240 milhões de mensagens foram relatadas de spam bloqueadas na caixa de entradas de usuário de e-mail.

Figura 6 – Estatística global de ameaças cibernéticas.

Fonte: Disponível em https://epocanegocios.globo.com/Tecnologia/noticia/2020/09/os-ataques-ciberneticos-explodem-durante-pandemia-e-expoem-vulnerabilidades-das-empresas.html

O mundo do cibercrime é muito eficiente pois estes invasores aproveitam da navegação anônima no espaço cibernético onde cada criminoso está em um ambiente livre, sem formas para rastrear endereço de IP ou localização local e não possui uma autoridade em exercer o poder suficiente para interromper a linha de tráfico. Os criminosos sentem à vontade em fazer o que quiser, como invadir contas de redes sociais (Instagram, facebook, twitter); atacar contas bancárias no exterior e aproveitar do uso de criptomoedas (MOURA; HAIDAR, 2020).

Com a pandemia do covid-19, as empresas optaram pelo trabalho remoto, de acordo com análise feita pelo Julius Baer, o crescimento de dispositivos pode chegar a 125 milhões de dispositivos conectados em 2022 de forma exponencial (MOURA; HAIDAR, 2020). A transferência das pessoas para o mundo digital ocasionou o grande fluxo de dispositivos conectados à internet, assim proporcionando a facilidade de ataques e favorecendo o comércio de crimes cibernéticos a crescer, pois o usuário não possui os conhecimentos necessários para manter os dispositivos protegidos.

Figura 7 – Dados de crescimento de números de dispositivos conectados ao espaço cibernético.

Fonte: Disponível em https://epocanegocios.globo.com/Tecnologia/noticia/2020/09/os-ataques-ciberneticos-explodem-durante-pandemia-e-expoem-vulnerabilidades-das-empresas.html

A técnica de *phishing*, relacionada a um trocadilho da palavra pesca, a prática consiste em jogar uma “isca”. Segundo Maldonado (2019), o WhatsApp foi a ferramenta no qual beneficiada para as práticas ilegais, muitas das vezes o autor se passa por uma instituição ou banco onde induz a vítima a preencher dados pessoais (nome, CPF, senhas, RG e etc.).

De acordo com pesquisa pelo grupo do PSafe (2017), possui outros tipos de fraudes com links maliciosos circulavam em grupos de redes sociais, muitos dos links compromete a vítima informando que a própria ganhou um iphone, roupas, sorteios, porém ao acessar o link, o indivíduo pode ser induzido a digitar informações pessoais a partir de engenharia social.

Figura 8 – Gráficos de principais ataques de *phishing*.

Fonte: Disponível em https://www.psafe.com/blog/ataques-ciberneticos-como-se-proteger/

4.1 Condições para prevenir de ameaças cibernéticas

Atualmente, a segurança trata-se de um termo essencial, porém é negligenciado em organizações, política e na sociedade devido à dificuldade de entender este tópico. “O único computador completamente seguro é o computador que ninguém consegue acessar”, frase dita pelo cientista da computação Willis Ware (1920), muitos acham que é apenas criar um ambiente para acesso à internet, sem configurar estrutura da rede, servidores, chaves criptográficas e então está seguro. Existem condições para manter a segurança e combater a ação de terceiro em ambientes corporativos e domésticos.

Para assegurar a proteção dos dados pessoais, o usuário pode adotar os seguintes métodos: Os softwares dos sistemas devem manter atualizados de acordo com as respectivas versões mais recentes distribuída pelos próprios fornecedores pois torna o sistema mais invulneráveis a ataques; É essencial possuir cópias de dados essencialmente importantes, pois caso um hacker invada o sistema e roubem, o usuário possui maneiras de recuperação. O usuário tem que lembrar de fazer backup; Os usuários devem criar senhas fortes com no mínimo 8 caracteres como é recomendado em sites onde exigem o *login*. Esta senha tem que apresentar misturas entre números, letras maiúscula e minúscula e caso insira caracteres especiais, a senha fica mais robusta de um terceiro descobrir; Tome cuidado ao utilizar wi-fi público, pois não possuem nenhum tipo de firewall ou tipo de segurança. Muito

comuns terceiros ter acesso de controle do local, por isso nunca utilize login ou senhas, contas de cartão de crédito em wi-fi de shopping, aeroporto e praças pois está correndo grande risco de privacidade; Não acesse links sem certificado de segurança na página da web, pois dará o passe para o invasor utilizar técnica de *phishing* ou instalar um *malware* e assim ter acesso respectivamente as informações do usuário; Para reforçar a proteção de contas ou informações nas nuvens, usuários devem configurar suas senhas com fator de autenticação duplo, as maneiras são a partir de token, pendrive ou digital, método mais tradicional atualmente, usado em smartphones. De exemplo é o Google, para impedir invasão de contas (e-mail, redes sociais e banco), o usuário pode usar este recurso para se manter protegido; Para empresas nas quais trabalham com dados sigilosos devem adquirir o uso de *Virtual Private Network* (Rede privada virtual) ou vpn. A vpn fornece uma conexão mais segura onde provedores de banda-larga e terceiros não conseguem ter acesso a pacotes de redes, escondendo o ip da máquina. Os usuários que utilizam vpn tornam "invisível na internet"; Qualquer usuário é necessário manter o antivírus ativo, pois o software faz varredura por busca de ameaças no disco rígido; rede; links provavelmente maliciosos ou sem certificado e caixa de entrada de e-mails. O Windows 10 já fornece um antivírus dentro do seu próprio sistema operacional, mas os usuários podem ficar à vontade para selecionar outros softwares (Avast, AVG, Bitdefender, Kaspersky etc.).

5. CONSIDERAÇÕES FINAIS

O resultado da pesquisa mostra que a pandemia é o período em que expôs as maiores vulnerabilidades tecnológicas do sistema. Desencadeando a ocorrências de crimes cibernéticos, apresentando diversidades e métodos de ataques com fator de ocorrência do distanciamento social em que ataquem perseguição de múltiplos alvos são direcionados a técnicas de engenharia social. O estudo concluiu que o crime cibernético está responsivo ao fato de trabalho remoto, fluxo de pessoas interconectadas no espaço cibernético e falta de conhecimento de segurança para retenção dos crimes.

O contexto da pesquisa bibliográfica demonstra o estudo de cibersegurança com ênfase em relação à encontrada mundialmente de 2020 – 2021. A limitação para o desenvolvimento foi realizada a partir de buscas de artigos, livros e noticiários. A maior

dificuldade foi reduzir o conteúdo extensivo na abordagem da pesquisa solicitada pelo instrutor.

No ponto de vista do autor, a chave para a segurança é treinar os profissionais em ordem deles ganharem o conhecimento necessário na proteção dos sistemas corporativos. Não vai adiantar empresas gastarem milhares de dólares, reais ou euro em tecnologia pois o quanto, mas tecnologia evoluem mais os métodos dos criminosos evoluem e tornam totalmente críticos.

6. REFERÊNCIAS

ALHAZMI, Omar; MALAIYA, Yashwant; RAY, Indrajit. Security vulnerabilities in software systems: A quantitative perspective. In: **IFIP Annual Conference on Data and Applications Security and Privacy**. Springer, Berlin, Heidelberg, 2005. p. 281-294.

AC Certificaminas. **Crescimento de crimes cibernéticos na pandemia: como não ser vítima.** 2021. Disponível em <https://cryptoid.com.br/identidade-digital-destaques/crescimento-de-crimes-ciberneticos-na-pandemia-como-nao-ser-uma-vitima/>. Acesso em 6. mai. 2021.

BALOCH. **Ethical Hacking and Penetration Test Guide.** Auerbach Publications, 2017.

BORKOVICH, Debra J.; SKOVIRA, Robert J. WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19. **Issues in Information Systems**, v. 21, n. 4, 2020.

CARREIRAS, Helena et al. Cibersegurança e ciberdefesa em tempos de pandemias. **IDN Brief**, 2020.

CIO. **EUA originam maior parte dos ciberataques contra a América Latina**. Disponível em <https://cio.com.br/noticias/eua-originam-maior-parte-dos-ciberataques-contra-a-america-latina/>. Acesso em 16. mai. 2021.

CONKLIN, WHITE, COTHREN, DAVIS, WILLIAMS **CompTIA Security+ All-In-One Exam Guide, fifth Edition (Exam Sy0-601))**. McGraw Hill, 2018

DANTAS, L. M. **Segurança da informação: uma abordagem focada em gestão de riscos.** Olinda, PE: Livro Rápido, 2011

DEMO, P. **Metodologia do conhecimento científico**. São Paulo: Atlas, 2000.

FERNANDES. A**. A. Implantando a governança de TI: da estratégia à gestão de processos e serviços.** Rio de Janeiro: Brasport, 2014.

FRAGA, Bruno. **Técnicas de Invasão**: Aprenda as técnicas usadas por hackers em invasões reais. Editora Labrador, v. 3, f. 148, 2019. 296 p.

FONTANILLA, M.V. Cybercrime pandemic. **Journal of Asian and International Bioethics,** Journal of Asian and International Bioethics, n. 30, p. 161-165, 4.mai. 2021.

FORTINET Resources. **Types of cyber Attacks**. Disponível em <https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks>. Acesso em 10. abr. 2021.

GEUS, Paulo Lício de; NAKAMURA, Emilio Tissato. Segurança de Redes em ambientes corporativos. São Paulo: Novatec, 2007.

HE, Ying et al. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. **Journal of medical Internet research**, v. 23, n. 4, p. e21747, 2021.

HENRIQUE PEDRO. **Você sabe a importância de ter um antivírus?** Disponível em <https://indicca.com.br/importancia-de-ter-um-antivirus>. Acesso 15. jun. 2022.

Jornal da Globo. <Ataques cibernéticos com pedidos de resgate triplicam durante a pandemia, aponta levantamento> 2021. https://g1.globo.com/jornal-da-globo/noticia/2021/05/15/ataques-ciberneticos-com-pedidos-de-resgate-triplicam-durante-a-pandemia-aponta-levantamento.ghtml>. Acesso em 18. abr. 2021.

KNIGHT, Peter T. **A internet no Brasil**: origens, estratégia, desenvolvimento e governança. Minnesota: AuthorHouse, 2014.

KRUSE, Clemens Scott et al. Cybersecurity in healthcare: A systematic review of modern threats and trends. **Technology and Health Care**, v. 25, n. 1, p. 1-10, 2017.

MALDONADO. **LGPD: Lei Geral de Proteção de Dados comentada**. Thomson Reuters. 2019.

MELO, Sandro. **Exploração de Vulnerabilidades em Redes TCP/IP**. 3º. ed. São Paulo: Alta Books, 2017. 640 p.

MEYERS. Mike **Meyers' CompTIA Security + Certification Guide, Third Edition (Exam Sy0-601)**. McGraw Hills, 2021

MILLER, L.C. **Cybersecurity for dummies**. New Jersey: Wiley, 2014. 76 p.

MOURA, HAIDAR. <Os ataques cibernéticos explodem durante pandemia e expõem vulnerabilidades das empresas> 2020. https://epocanegocios.globo.com/Tecnologia/noticia/2020/09/os-ataques-ciberneticos-explodem-durante-pandemia-e-expoem-vulnerabilidades-das-empresas.html. Acesso em 21. mar. 2021.

MUGGAH. **O problema do cibercrime no Brasil**. 2015. Disponível em <https://brasil.elpais.com/brasil/2015/10/23/opinion/1445558339_082466.html>. Acesso em 5. mar. 2021.

NAKAMURA, GEUS. **SEGURANÇA DE REDES EM AMBIENTES COOPERATIVOS.** Rio de Janeiro. Novatec, 2010.

PATRIARCA PAOLA. **Golpe do emprego sms com oferta de trabalho para o Sebrae chama atenção de internautas e reacende alerta**. Disponível em <https://g1.globo.com/tecnologia/noticia/2022/03/22/golpe-do-emprego-sms-com-oferta-de-trabalho-para-o-sebrae-chama-atencao-de-internautas-e-reacende-alerta.ghtml>. Acesso em 22. mai. 2022.

PortNet. **Por que hackers são mais temidos por empresas que inflação e austeridade?** Disponível em <https://www.portnet.com.br/por-que-hackers-sao-mais-temidos-por-empresas-que-inflacao-e-austeridade/>. Acesso em 13. abr. 2021.

PRANGGONO, Bernardi; ARABO, Abdullahi. COVID-19 pandemic cybersecurity issues. **Internet Technology Letters**, v. 4, n. 2, p. e247, 2021.

PSAFE. **Ataques cibernéticos: O que é e como se proteger.** 2017. Disponível em <https://www.psafe.com/blog/ataques-ciberneticos-como-se-proteger/>. Acesso em 2. mar. 2021.

REISSWITZ, F. **Análise de sistemas.** Joinville: Clube de Autores, 2012. v. 2

RIBEIRO GABRIEL. **Por que a pessoa que te aplica golpe pelo WhatsApp nunca é presa no Brasil?** Disponível em <https://www.uol.com.br/tilt/noticias/redacao/2018/02/05/por-que-a-pessoa-que-tenta-te-roubar-pelo-whatsapp-nao-e-presa-no-brasil.html>. Acesso em 8. mai. 2021.

SEVERINO, A. J. Metodologia do trabalho científico. São Paulo: Cortez, 2007.

VELASCO CLARA, MANCINI FERNANDO. **Golpes em redes sociais crescem no Brasil?** Disponível em <https://g1.globo.com/economia/tecnologia/noticia/2022/03/09/golpes-em-redes-sociais-crescem-no-brasil-veja-como-nao-cair.ghtml>. Acesso 20. mai. 2022.

WILLIAMS, Christina Meilee; CHATURVEDI, Rahul; CHAKRAVARTHY, Krishnan. Cybersecurity risks in a pandemic. **Journal of Medical Internet Research**, v. 22, n. 9, p. e23692, 2020.

WILLIAMS MIKE. **Everything you need to know about Virtual Private Networks. <**https://www.techradar.com/vpn/virtual-private-networks>. Acesso 15.jun.2022.