OS RISCOS OFERECIDOS POR HACKERS NÃO-ÉTICOS E A IMPORTÂNCIA DA CIBERSEGURANÇA ATUALMENTE

BOLSISTA: JOSÉ CAINAN JANSEN CUNHA[1]

VOLUNTÁRIO: FILIPE MENDES SILVA[2]

ORIENTADOR: LUIS FERNANDO MAIA[3]

[1] José Cainan Jansen Cunha, Ciência da Computação, IFMA-Campus Caxias, cainanjose@acad.ifma.edu.br

[2] Filipe Mendes Silva, Ciência da Computação, IFMA-Campus Caxias, mendesfilipe@acad.ifma.edu.br

[3] Doutor Luís Fernando Maia, IFMA-Campus Caxias, luis.maia@ifma.edu.br

Caxias – MA

Início da Execução: 01/09/2023

Resumo:

Justifica-se a importância de tal pesquisa devido principalmente o aumento exponencial do uso da internet, redes sociais, e a migração de dados do meio físico para o meio digital, baseado nisso é necessário mostrar a vulnerabilidade cibernética da sociedade como um todo. Dessa forma, o presente trabalho teve como objetivos: Analisar a vulnerabilidade dos indivíduos e os riscos oferecidos pelos hackers atualmente, mapear os principais alvos de hackers na atualidade e investigar o interesse pela área de cibersegurança por parte da comunidade da computação, a abordagem quantitativa foi escolhida para analisar os dados provenientes dos questionários, entretanto devido à falta de um parecer do comitê de ética de pesquisa, seja ele positivo ou negativo, os questionários até o presente momento não foi aplicado. Porém um breve um levanto de pesquisas e artigos anteriores com o foco em hackers mostram que a sociedade brasileira em geral é sim vulnerável a ataques cibernéticos.

Palavras-chave: Vulnerabilidade, Hackers, Cibersegurança, Sociedade brasileira, Ataques cibernéticos.

Financiamento: O projeto foi financiado pela Fundação de Amparo à Pesquisa e ao Desenvolvimento Científico e Tecnológico do Maranhão (FAPEMA).

1 - Introdução

Atualmente o mundo a chamada “era digital” ou “era informação” tal era começou logo após a era industrial, que pegou impulso já na Primeira Revolução Industrial com seus avanços tecnológicos, a era digital é marcada principalmente por otimizar o fluxo de informações e cibernetização de dados. Devido a migração de dados do meio físico para o meio digital surgiu uma vulnerabilidade desses dados, informações que antes eram mais difíceis de um indivíduo mal intencionado ter acesso, hoje com a digitalização essas informações estão à mercê dos famosos hackers.

Uma das consequências dessa digitalização foi a vulnerabilidade dos dados, como já citado, nos dias atuais praticamente toda a sociedade vive dependente das redes sociais, bancos digitais, streamers e outros apps que tem acesso a informações pessoais e dados bancários, principalmente pessoas da geração Z, pessoas nascidas entre 1997 e 2012, essa geração, é marcada por ter mais acesso à tecnologia e por sua vez ser também mais dependente, o que termina por aumentar a sua vulnerabilidade a ataques hackers.

Embora hoje em dia o termo hackers seja constantemente associado a criminosos, a sua origem é completamente diferente, o termo surgiu entre 1950 e 1960 no instituto de Tecnologia de Massachusetts (MIT), não muito tempo depois o jornalista Steven Levy introduziu em seu livro, Hackers: heroes of the Computer Revolution, o termo ética hacker. Segundo Levy, hackers éticos buscam fortalecer uma rede ou um sistema contra hackers mal-intencionados, investigando e analisando os softwares em busca de pontos fracos, com tal definição vale salientar que embora as áreas da computação como, engenharia de software, arquitetura de computadores, análise e desenvolvimento de sistemas e ciência da computação, sejam áreas mais buscadas nos anos 2000, uma carreira ainda pouco procurada é a de hackers profissionais (hackers éticos). Diante desse panorama cabe uma simples pergunta: qual o nível de vulnerabilidade da sociedade.

Portanto, a presente pesquisa teve como objetivo analisar a vulnerabilidade dos indivíduos e os riscos oferecidos por hackers não éticos no cenário atual, tendo como objetivos especifico, mapear os principais alvos da atualidade; demonstrar maneiras de evitar torna-se vítima de crimes cibernéticos e investigar o interesse pela área da segurança da informação.

2 – Materiais e Métodos

2.1 Materiais

- Artigos e pesquisas cientificas publicados nos últimos 20 anos, focados principalmente em segurança cibernética.
- Questionário desenvolvido com perguntas de perguntas objetivas, destinado a indivíduos de 18 anos em diante.
- Plataforma Microsoft forms, usada para a elaboração e aplicação dos questionários.
- Documento oficial para os participantes assinarem, garantindo o consentimento para o uso dos dados fornecidos
- Softwares para a criação, aplicação e análise dos dados coletados, exemplo, Microsoft forms.
- Documentação necessária para a submissão ao Comitê de Ética em Pesquisa, incluindo formulários de submissão.

2.2 Métodos

Durante a execução da presente pesquisa foi decidido uma abordagem quantitativa, devido ao fato de que um dos objetivos é analisar a vulnerabilidade cibernética da sociedade atualmente, com o intuito de gerar dados a respeito de possíveis ataques na qual estão sujeitos. Essa metodologia foi dividida em; revisão bibliográfica, submissão ao comitê de ética, aplicação dos questionários e coleta de dados, analises dos dados coletados, discussão dos resultados e o relatório final. De início a revisão bibliográfica foi feita baseada em autores que alertam sobre os perigos de hackers não éticos e como evitar ataques.

O projeto foi submetido ao Comitê de Ética em Pesquisa, em vista que envolve a coleta de dados de seres humanos. Porém até o momento da produção desse relatório não foi recebido um parecer do Comitê, seja ele positivo ou negativo, diante disso, foi decidido realizar um levantamento de outras pesquisas artigos e reportagens anteriores, afim de se chegar a um resultado preliminar, enquanto é aguardado um retorno do comitê de ética, entretanto o questionário já foi desenvolvido, mas não aplicado.

Segue o questionário:

1- ***O que vem em sua mente quando ouve falar em hackers?***

- a) Alguém que invade sistemas para benefício próprio
- b) Um criminoso que pratica crimes cibernéticos
- c) Alguém que rouba dados pessoais para chantagem
- d) Alguém que trabalha protegendo uma empresa contra ataques cibernéticos

2- Você acha que os hackers atualmente possuem alguma importância para a sociedade?

- a) Hackers são criminosos, logo não contribuem para a sociedade de forma positiva
- b) Sim, hackers não são puramente criminosos
- c) Não sei/Neutro

3-Geralmente, você ouve mais coisas positivas ou negativas sobre os hackers?

- a) Positivas
- b) Negativas
- c) Neutro

4-Você acha que é possível trabalhar como hacker e ganhar dinheiro legalmente?

- a) Não, não existe emprego para hacker
- b) Sim, mas não ganha muito
- c) Não, pois ser hacker é crime
- d) Sim, e acho que ganha bem
- e) Não sei/Neutro

5-Você acredita que a mídia influencia na percepção das pessoas sobre os hackers?

- a) Sim, a mídia frequentemente retrata hackers de maneira negativa
- b) Não, a mídia não influencia minha opinião sobre hackers
- c) Não tenho certeza

6-Você considera a educação em segurança cibernética importante para a prevenção de crimes online?

- a) Sim, é fundamental para a proteção pessoal e da sociedade
- b) Não, não vejo a necessidade de aprender sobre segurança cibernética
- c) Não sei/Neutro

7-Você já ouviu falar sobre hackers éticos?

- a) Sim, estou familiarizado(a) com esse termo
- b) Não, nunca ouvi falar
- c) Não tenho certeza

8-Você acredita que aprender habilidades de segurança cibernética é importante para proteger suas informações online?

- a) Sim, é essencial
- b) Não, não vejo a necessidade
- c) Não tenho certeza

9-Você costuma compartilhar senhas ou informações pessoais online com amigos?

- a) Sim, compartilho ocasionalmente
- b) Não, nunca compartilho informações pessoais
- c) Não sei/Não tenho certeza

10-Você acredita que é importante ter cuidado ao clicar em links ou baixar arquivos da internet para evitar ameaças cibernéticas?

- a) Sim, sempre sou cauteloso(a)
- b) Não, não acho que seja tão importante
- c) Não tenho certeza

11-Você utiliza regularmente antivírus ou programas de segurança em seus dispositivos (computador, smartphone, etc.)?

- a) Sim, sempre mantenho meus dispositivos protegidos
- b) Não, não costumo utilizar programas de segurança
- c) Não sei/Não tenho certeza de como fazer isso

12-Como você reage ao receber mensagens ou solicitações de amizade de desconhecidos em suas redes sociais?

- a) Aceito todas as solicitações
- b) Aceito apenas de pessoas que conheço pessoalmente
- c) Ignoro solicitações de desconhecidos

3 – Resultados

Analisando um trecho da dissertação de Vera Lúcia Viveiros de Sá, Hackers: Mocinhos e Bandidos, Estudo de grupos brasileiros desfiguradores de sites, quando o desfigurador altera uma homepage, ele busca fama, querendo que todos vejam sua obra. Se o site alterado for de uma grande empresa, tanto na área relacionada à Internet quanto fora dela, isso causará uma grande repercussão, pois o ataque será divulgado por algum meio de comunicação. Por esse

motivo, os alvos preferenciais são os sites das grandes corporações. Ocorre uma disputa declarada entre os desfiguradores e os especialistas em segurança das empresas. O defacer está sempre de olhos bem abertos para os "grandes sites", mas se o servidor de uma pequena empresa cruzar com ele, o ataque também ocorrerá (Viveiros, 2005, p.28), percebe-se que qual um pode ser um eventual alvo para os desfiguradores (hackers não-éticos). Diante desse panorama, é notório uma certa vulnerabilidade, visto que embora hackers tenham certas preferências para seus ataques, não existem restrições para seus alvos.

Vale salientar ainda que Steven Levy, jornalista citado anteriormente, estabeleceu 3 gerações de hackers em seu livro, Hacker: heores of the Computer Revolution, ele descreve a primeira como: Hackers de Hardware e Mainframes (1950 – 1960) essa geração era motivada pelo aprendizado, a eficiência e a elegância do código, essa geração seguia o que Levy chamava de ética hacker. A segunda geração: Hackers de jogos e PCs (1970 - 1980), era motivada por criar softwares úteis, com ênfase no desenvolvimento de jogos e aplicações inovadoras, um grande representante dessa época foi Steve Wozniak. Por fim a terceira geração: Hackers de rede (1980 - atualmente), nessa geração os hackers são incentivados principalmente por questões éticas e políticas. A partir da terceira geração os hackers ganharam a fama que têm hoje.

Na pesquisa Hackers e suas Características de Juliano Vieira da Rocha, afirma-se que o Brasil ainda está preparado para entender os crimes cibernéticos, seja tecnologicamente, boas práticas, processos e em relação as leis, para defender a sociedade em geral. Com mais uma pesquisa adicionando peso ao argumento que a sociedade brasileira como um todo, é fraca ciberneticamente falando, não resta muitas dúvidas de tal vulnerabilidade. Porém para uma visão mais atualizada, foi pensado a realização do questionário mostrado anteriormente.

4- Bibliografia

Sá, Vera Lúcia Viveiros. HACKERS: MOCINHOS E BANDIDOS Estudo de grupos brasileiros desfiguradores de Sites. Disponível em: http://www.bdae.org.br/dspace/handle/123456789/2208 acesso em: 10 de jun. 2024

Rocha, Juliano Vieira da. Hackers e suas Características. Disponível em: https://www.academia.edu/27538027/HACKERS_e_suas_características . Acesso em: 15 jun. 2024

SOUZA, Ivan de. HACKER: o que é, o que ele faz e como consegue atacar o seu site - https://rockcontent.com/br/blog/hacker/ . Acesso em 20 de fev. De 2023.

ESTRELA, Sidney. HACKERS: quem são e como se proteger adequadamente? - https://www.certifiquei.com.br/hackers/#:~:text=O%20principal%20perigo%20para%20as,econômicos%2C%20morais%20e%20de%20imagem . Acesso em 25 de fev. De 2023.

LOPES, Leonardo. Principais vantagens da tecnologia para vida moderna - https://www.migalhas.com.br/depeso/342894/principais-vantagens-da-tecnologia-para-a-vida-moderna . Acesso em 05 de ago. De 2024.

LEVY, Steve. Hackers: Heroes of the Computer Revolution. Nova York, 1984.

5- Agradecimentos

Luís Fernando Maia (orientador), José Cainan Jansen Cunha (bolsista), Filipe Mendes Silva (voluntário). Agradeço ainda a Fundação de Amparo à Pesquisa e ao Desenvolvimento Científico e Tecnológico do Maranhão (FAPEMA), que realizou o financiamento para a realização dessa pesquisa.