SEGURANÇA DA INFORMAÇÃO: DESENVOLVIMENTO DE UMA EXTENSÃO PARA O NAVEGADOR GOOGLE CHROME QUE IMPEDE ATAQUES DE PHISHING

Categoria do Trabalho – Apresentação Oral

Dhyonatan Santos de Freitas, Gustavo Baumrucker Maertner e Victor Gonçalves da Luz

Centro Universitário SENAI Santa Catarina - UniSENAI - Campus Joinville

dhyonatan.freitas@edu.sc.senai.br

RESUMO

Este trabalho aborda o desenvolvimento de uma extensão para navegadores de internet visando prevenir ataques de *phishing*. A metodologia engloba descrição do projeto, tecnologias utilizadas e validação da ferramenta pelos usuários. Resultados demonstram eficácia na identificação de URLs maliciosas e alta aceitação dos usuários. Considera-se a extensão uma ferramenta promissora na proteção contra *phishing*, oferecendo uma solução acessível e eficaz para mitigar riscos na navegação web.

Palavras-chave: *Phishing*; Engenharia Social; Segurança da Informação; e Extensão de Navegador.

INTRODUÇÃO

A tecnologia da informação vem ganhando cada vez mais importância, tornando-se um dos setores mais importantes economicamente de um país de acordo com Kohn e Moraes (2007). Com isso, percebe-se que existe uma preocupação global em relação à segurança das informações manipuladas pelos usuários. No que se refere ao uso de tecnologias para proteção das informações, a área de pesquisa e desenvolvimento já está bastante consolidada (DE LEMA; CARPEGGIANI; FREITAS, 2021). No entanto, infratores estão buscando alternativas

para enganar os usuários ao invés das próprias ferramentas de proteção. Esse movimento é conhecido como engenharia social.

A engenharia social engloba métodos de distorções cognitivas para conseguir dados sigilosos, senhas, dados bancários e outros sistemas protegidos de empresas, usuários e instituições, utilizando conhecimentos empíricos e científicos aplicados de um modo sociável de acordo com as necessidades humanas (AVANCI, L; VICENTINE, A; RIZO, A; 2021). Atualmente são utilizadas algumas técnicas de coerção que se baseiam nos conceitos da engenharia social, entre elas o envio de emails, URLs, mensagens de celular e até mesmo ligações telefônicas de forma mal intencionada.

Para evitar esse tipo de situação, engenheiros e desenvolvedores de software têm reunido esforços para desenvolver mecanismos de proteção para esse tipo de ataque. Estes mecanismos podem ser construídos utilizando infraestrutura em hardware, providenciando filtros chamados de *Proxys* e *Firewalls*. Além disso, na camada de aplicação, também tem-se notado esforços no desenvolvimento de aplicações web que funcionam da mesma forma (LOURENÇO, M; DUARTE, R.; 2020).

A Federação Brasileira de Bancos (FEBRABAN) realizou um estudo que aponta que o Brasil registrou um aumento de 80% nas tentativas de ataques de *phishing* com intuito de roubo financeiro (BORGES, A; 2020). *Phishing* é uma forma de engenharia social que busca explorar as fraquezas encontradas nos processos, principalmente de empresas, causadas pelos próprios usuários. Por exemplo, um sistema pode ser tecnicamente seguro contra ameaças, furto de senhas e logins, porém os usuários finais podem acabar vazando as senhas deles caso um golpista peça para que ele atualize sua senha via um protocolo HTTP, o que no fim acaba comprometendo a segurança do sistema por completo.

O Cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), entidade responsável pela análise e monitoramento dos ataques cibernéticos no território brasileiro, divulgou recentes estatísticas evidenciando um notório aumento nos incidentes de *phishing*. No decorrer do ano de 2023, foram reportados 32.317 casos de *phishing* no Brasil. Em contraste com outras modalidades de ataques, por exemplo o Malware, constata-se que os ataques de *phishing* apresentam uma frequência cinquenta vezes superior. Esta discrepância é

atribuída pelo Cert.br às particularidades inerentes ao *phishing*, cujo objetivo reside na exploração direta da engenharia social das potenciais vítimas ao invés de atacar o próprio sistema (CERT.BR, 2024).

Neste contexto, o objetivo geral deste trabalho é desenvolver um *add-on* (extensão ou plugin) para navegadores de internet baseados na arquitetura Chrome, que tem como função coibir ataques de *phishing*, impedindo que usuários acessem sites maliciosos durante a navegação na internet.

METODOLOGIA

A metodologia deste trabalho abrange a descrição detalhada do projeto de software, das tecnologias empregadas, da arquitetura do software e a validação da ferramenta por parte dos usuários.

Diversas tecnologias foram empregadas para o desenvolvimento da extensão, com destaque para o uso do Google Chrome devido à sua ampla adoção e disponibilidade de extensão na Chrome Web Store. As linguagens de programação utilizadas foram o PHP na versão 7.4, para consultas em servidores externos e manipulação de arquivos de texto; JavaScript na versão ES2015, para validações locais sem a necessidade de conexão externa; HTML na versão 5 e CSS na versão 3, responsáveis pelo desenvolvimento da interface do usuário.

A arquitetura da extensão segue as etapas básicas de entrada, processamento e saída de um software. Na etapa de entrada, URLs acessadas pelos usuários durante a navegação na internet são capturadas. O processamento envolve a validação dessas URLs, com base em duas listas: *Blacklist*, contendo URLs consideradas inseguras, e *Whitelist*, com URLs conhecidas por serem seguras. Estas listas são atualizadas manualmente pelos administradores conforme novas informações são obtidas.

Após a verificação das listas *Blacklist* e *Whitelist*, a extensão verifica se a URL possui certificado de segurança HTTPS (protocolo de segurança criptografado), notificando o usuário caso contrário. Em seguida, verifica o domínio da URL para determinar sua confiabilidade, considerando seu país de origem e histórico de atividades maliciosas. Finalmente, utiliza-se

uma API (conjunto de regras e protocolos) para consultar a ferramenta WhoIs (DAIGLE, L; 2004), que fornece informações sobre o registro do domínio, como data de registro e associação a CPF ou CNPJ, garantindo maior confiabilidade na análise da extensão.

Este processo de validação em camadas permite uma abordagem abrangente para identificação e prevenção de ataques de *phishing*, fornecendo aos usuários um mecanismo robusto de proteção durante sua navegação na internet.

RESULTADOS E DISCUSSÕES

Após o desenvolvimento e implementação da extensão, bem como a avaliação por parte dos usuários, foram obtidos resultados significativos que contribuem para a compreensão da eficácia e usabilidade da ferramenta.

Em relação ao processo de download e instalação da extensão, este se mostrou simplificado e acessível aos usuários por meio da Chrome Web Store, onde a extensão foi publicada. A maioria dos participantes concordou que o processo de instalação foi fácil e direto, destacando a acessibilidade da extensão aos usuários finais.

A etapa de configuração da extensão permitiu aos usuários personalizar o funcionamento de acordo com suas preferências, como habilitar ou desabilitar a validação para sites sem certificado HTTPS e a verificação do WhoIs. Esta flexibilidade na configuração foi bem recebida pelos usuários, facilitando a adaptação da extensão às suas necessidades individuais.

Durante a navegação na internet, a extensão mostrou-se eficaz na identificação e bloqueio de URLs maliciosas que poderiam conter ataques de *phishing*. A maioria dos usuários considerou os alertas da extensão claros e intuitivos, facilitando a compreensão dos riscos associados aos sites bloqueados. No entanto, houve uma parcela de participantes que indicou que a extensão poderia ser mais efetiva na prevenção do acesso a sites duvidosos, sugerindo a implementação de Blacklists alimentadas por empresas renomadas em segurança da informação.

Apesar dessas observações, a grande maioria dos usuários afirmou que continuaria a utilizar a extensão e a recomendaria a outras pessoas, indicando um alto nível de aceitação e potencial

escalabilidade no contexto dos usuários. Entretanto, algumas melhorias na simplicidade e usabilidade da extensão foram sugeridas para garantir uma experiência mais fluida e livre de incômodos para os usuários finais.

Esses resultados indicam que a extensão desenvolvida possui uma base sólida, mas ainda há espaço para refinamentos e otimizações que podem aumentar ainda mais sua eficácia e aceitação entre os usuários.

CONSIDERAÇÕES FINAIS

Os ataques de *phishing* representam uma ameaça significativa para organizações e usuários individuais, explorando a ingenuidade humana para comprometer a segurança dos sistemas computacionais. A conscientização dos usuários sobre esses ataques por meio de treinamentos é uma estratégia fundamental na mitigação desses riscos, complementada pelo desenvolvimento e implementação de tecnologias de proteção.

Este trabalho teve como objetivo principal desenvolver uma ferramenta para auxiliar os usuários finais na proteção contra tentativas de *phishing*. A extensão desenvolvida para o Google Chrome demonstrou eficácia em validar URLs e alertar os usuários sobre possíveis ameaças, proporcionando uma camada adicional de segurança durante a navegação na internet.

Os resultados dos testes realizados com a extensão indicam que ela é capaz de prevenir ataques de *phishing* para URLs conhecidas e armazenadas na Blacklist. Além disso, as configurações da extensão funcionam de maneira adequada, garantindo que ela não interfira na experiência de navegação do usuário, mas sim o auxilie na proteção de seu dispositivo.

Destaca-se também a velocidade da extensão em suas rotinas de validação, que intercepta as páginas antes mesmo de serem completamente carregadas, redirecionando o usuário para uma página segura, sob seu controle. Esse processo contribui significativamente para a redução do risco de exposição a sites maliciosos.

Por fim, a extensão desenvolvida demonstrou-se uma ferramenta promissora na proteção contra ataques de *phishing*, fornecendo uma solução acessível e eficaz para mitigar os riscos associados a esse tipo de ameaça na internet.

REFERÊNCIAS

BORGES, João. Conheça as tentativas de golpes financeiros mais comuns na pandemia e saiba como evitá-los. Febraban, 2020. Disponível em: https://portal.febraban.org.br/noticia/3522/pt-br/. Acesso em: 15 Set. 2023.

CERT.BR. Estatísticas de Incidentes de Segurança no Brasil. Disponível em: https://stats.cert.br/incidentes/. Acesso em: 09 Abr. 2024.

DAIGLE, Leslie. WHOIS protocol specification. 2004.

DE LEMA, Markus Carpeggiani; FREITAS, Marcio. ATAQUES RANSOMWARE. Seminário de Tecnologia, Gestão e Educação, v. 3, n. 1, 2021.

DE SOUZA PEREIRA, Lucas Avanci; VICENTINE, Augusto Luciano; RIZO, Andre Castro. Impactos da engenharia social na segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 4, n. 1, p. 48-58, 2022.

KOHN, Karen; MORAES, CH de. O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital. In: XXX Congresso Brasileiro de Ciências da Comunicação. sn, 2007. p. 1-13.

LOURENÇO, Rogerio Marcos; DUARTE, Ruan Pereira. Gestão de segurança da informação. 2020.