josif 2023
15ª JORNADA CIENTÍFICA E TECNOLÓGICA
12º SIMPÓSIO DE PÓS-GRADUAÇÃO
DO IFSULDEMINAS
REALIZAÇÃO INSTITUTO FEDERAL Sul de Minas Gerais
APOIO FAPEMIG CNPq

SEGURANÇA DE SOFTWARE: ameaças e medidas de proteção

Daniel Augusto de M. Pedro

RESUMO

A revisão da literatura destaca a importância das medidas de segurança, explicando o funcionamento de alguns spywares tendo como base a prevenção dessas ameaças. O Brasil lidera a América Latina em ataques de spywares, visando o roubo de dados. Um estudo revelou as senhas mais comuns e vulneráveis usadas globalmente. Todos, desde desenvolvedores a usuários finais, devem se preocupar com a segurança de software, abordando aspectos técnicos e políticas de segurança de forma abrangente.

Palavras-chave: Tecnologia; Vulnerabilidades; Spywares.

1.INTRODUÇÃO

A segurança de software é um tema cada vez mais relevante na atualidade, devido à crescente dependência de tecnologias de informação e comunicação (TICs) em nossas vidas cotidianas. No entanto, a segurança de software não é um tema novo, e as ameaças cibernéticas sempre existiram desde o surgimento da internet. Segundo Santos e Silva (2022) com notabilidade de informações pessoais, houve um aumento de notícias relacionadas a crackers, Massachusetts Institute of Technology (MIT) publicou no Journal of Data and Information Quality da ACM (Association for Computing Machinery 2021) os vazamentos de dados no Brasil tiveram um aumento significativo de 493%.

Neste artigo científico, serão discutidas as principais ameaças cibernéticas e medidas de proteção para garantir a segurança do software.

2.FUNDAMENTAÇÃO TEÓRICA

Conforme Yamagawa (2015), quando se tem em mente criar um sistema, estão integradas a segurança física e a segurança lógica. A segurança de software pode ser definida como a proteção de dados e informações armazenados em um sistema computacional contra acesso não autorizado, uso indevido ou alteração.

Tendo como lógica as informações acima, o processo de controle de acesso bem implementado em um software garante maior segurança ao desenvolvedor e para o usuário. O mesmo ao ser aplicado restringe o acesso a certas funcionalidades, recursos e informações apenas a usuários autorizados.

Segundo Júnior (2013) hoje em dia, existem várias fragilidades como por exemplo falta de verificação de limites de alocação de memória, falta de validação na entrada de dados, falha na abertura de arquivos, finalização incorreta de uma conexão com um banco de dados, entre muitas outras. Para Correia e Sousa (2008) tem-se que qualquer pacote de software possui entre cinco a cinquenta bugs a cada mil linhas e código. Em meio a isso, algumas são vulnerabilidades.

Para combater essas vulnerabilidades, é importante realizar testes de segurança regularmente, usar técnicas de codificação segura e manter-se atualizado com as correções de segurança.

O método de defesa Estática tem como objetivo mitigar ou impedir ataques que ferem o sigilo de um sistema, em outras palavras ela tem como objetivo dizer se a integridade de um programa pode ser violada.

Já a Dinâmica tem como objetivo rodar o programa com um conjunto provável de entradas e analisar seu comportamento, tem como vantagem o benefício de analisar informações disponíveis em tempo real.

A análise manual (ou auditoria de código) se destina a descobrir vulnerabilidades de programação e também é útil para detectar vulnerabilidades de projeto.

3.MATERIAL E MÉTODOS

Para avaliar a eficácia das medidas de segurança, foi realizada uma revisão da literatura sobre as principais ameaças cibernéticas, ameaças de software e medidas de proteção a fim evitar certos *spywares* que são populares no Brasil, como o caso de Trojans e Keyloggers onde são programas de fácil instalação e executam tarefas simples como memorização de teclas digitadas e execução de tarefas maliciosas sem consentimento do usuário o levando a danos financeiros ou até mesmo danos reputacionais.

4.RESULTADOS E DISCUSSÕES

A revisão da literatura identificou que a maioria das ameaças cibernéticas e de software pode ser evitada ou mitigada por meio de medidas de segurança adequadas, incluindo firewalls, criptografia, técnicas de codificação segura e políticas de segurança, incluindo testes. De acordo com Ribeiro (2019) para a matéria do site TechTudo, o Brasil é o país da América Latina com maior número de ataques de *spywares* (27%), tendo como foco a instalação de programas com Trojans e Keyloggers para roubos de dados e credenciais bancárias. Uma boa proteção começa por senhas fortes e conhecimento prévio de como são os meios de propagação dos vírus virtuais. De acordo

com Marino (2020), em seu estudo são apresentados os resultados obtidos pela equipe de pesquisa da SafetyDetectives, que analisou um conjunto de mais de 18 milhões de senhas. Eles identificaram as 30 senhas mais comuns, previsíveis e, por último, as senhas mais frequentemente alvo de ataques no mundo, essas senhas se baseiam em várias utilizações desde aplicativos bancários até para acesso a redes sociais (FIGURA 1).

Figura 1 – Relatório das 30 senhas mais utilizadas no mundo

Fonte: MARINO, 2020

No entanto, é importante ressaltar que a segurança de software não é uma solução única e definitiva. As ameaças cibernéticas estão em constante evolução, e as medidas de segurança devem ser atualizadas regularmente para acompanhar as novas ameaças. Além disso, a segurança de software deve ser uma preocupação de todos os usuários, desde desenvolvedores até usuários finais, e deve ser abordada de forma abrangente, incluindo aspectos técnicos e políticas de segurança.

5.CONCLUSÕES

A segurança de software é um tema crítico na atualidade, e as ameaças cibernéticas podem ter graves consequências, incluindo roubo de dados, danos financeiros e reputacionais. No entanto, existem medidas de proteção eficazes que podem ser adotadas para minimizar essas ameaças. É importante que desenvolvedores, empresas e usuários finais sejam proativos em relação à segurança de software, adotando técnicas de codificação segura, políticas de segurança e conscientização do

usuário. Além disso, é crucial manter-se atualizado com as novas ameaças cibernéticas e atualizar regularmente as medidas de segurança para garantir a proteção adequada de dados e informações.

REFERÊNCIAS

CORREIA, M. P.; SOUSA, P. J. Segurança no software. Lisboa/PT: FCA, 2008.

MARINO, M. A 20 senhas mais hackeadas do mundo: A sua está aqui? Disponível em: . Acesso em: https://www.safetydetectives.com/blog/the-most-hacked-passwords-in-the-world/ Acesso em: 10 de junho de 2023.

RIBEIRO, Carolina. O Brasil é o principal alvo de spywares que roubam dados bancários. TechTudo, Parauapebas, 22 de out. de 2019. Disponível em: <https://www.techtudo.com.br/noticias/2019/10/brasil-e-principal-alvo-de-spywares-que-roubam-dados-bancarios.ghtml>. Acesso em: 12 de junho de 2023.

YAMAGAWA, R. Y. **Benefícios do teste na segurança do software**, 2015. Trabalho de conclusão de curso (Curso de Tecnologia em Análise e Desenvolvimento de Sistemas) - Faculdade de Tecnologia de Americana, Americana, 2015. Disponível em: http://ric.cps.sp.gov.br/handle/123456789/451. Acesso em: 10 de junho de 2023.