Ataque a redes abertas com *Man in the Middle*

Daniel da Silva de Paula Filho; Isabella da Cruz Prates; Lucas Rosa Alves; Lucas de Araujo Oliveira.
Instituto Federal de São Paulo. filho.dani@hotmail.com
Palavras-chave: Segurança da informação, Ataques cibernéticos, Redes abertas, Man in the Middle

Introdução

Buscando entender o funcionamento do ataque cibernético *Man in the Middle* a redes abertas, essa pesquisa analisa a execução do *cyberattack*, além de sugestões para prevenção de eventos desta natureza, já que mesmo com o devido cuidado, serviços que utilizam dados sensíveis fazem cada vez mais parte do cotidiano das pessoas, enquanto simultaneamente, os ataques cibernéticos aumentaram em 94% no Brasil e foi registrado 31,5 bilhões de tentativas de ataques no primeiro semestre deste ano (OLIVEIRA, 2022).

Objetivos

O objetivo desta pesquisa foi analisar o processo de um ataque *Man in the Middle* a redes abertas, como *Wi-Fi* livre, observando o encadeamento utilizado para o ganho do acesso e os pontos detentores de possíveis vulnerabilidades, possibilitando *logins* e ações maliciosas à vítima. Ademais, através de uma pesquisa de campo observar a desinformação ou o não uso de mecanismos preventivos mediantes a possíveis ataques.

Material e Métodos

A conexão sem fio hoje em dia é a forma mais popular de rede para os usuários porque oferece mais agilidade de uso. Milhões de pessoas usam redes sem fio para trabalhar, estudar ou apenas navegar na Internet em todo o mundo. Apesar do fato de que tudo é transmitido ao ar livre e pode ser interceptado por usuários mal-intencionados.

Os atuais métodos de proteção *Wi-Fi* podem conceder um nível de segurança adequado para a maioria dos utilizadores contendo a maioria dos ataques. Entretanto, existem alguns ataques que não podem ser bloqueados por tais mecanismos de segurança, esses ataques são chamados de ataques MITM *(Man-In-The-Middle Attack)* ou invasor no meio na tradução (KAPLANIS, 2015).

O ataque MITM é um dos ataques mais conhecidos na segurança de computadores, representando uma das maiores preocupações dos profissionais de segurança. O MITM visa os dados reais que fluem entre os terminais e a confidencialidade e integridade dos próprios dados (CONTI; DRAGONI; LESYK, 2016).

Conforme mostrado na Figura 1 a seguir, o ataque ocorre quando o invasor consegue por meio de ferramentas se passar pelo *gateway* de uma rede local, e infectar um dispositivo, se colocando entre o usuário e o serviço em que ele quer utilizar para obter informações, já que para o mesmo ele seria uma espécie de administrador da rede agora, e todas as informações passariam por ele.

Figura 1: Exemplo de um ataque MITM

Fonte: Adaptado de (ATAQUE, 2022)

Para prevenção é sugerido utilizar redes abertas apenas com a não submissão de nenhum dado sensível, como por exemplo, iniciar novas seções em redes sociais ou efetuar transações bancárias. Não utilizar senhas fáceis de adivinhar, como nomes e idade, pois são facilmente descobertas por programas automatizados de coleta de senhas, além de não utilizar a mesma senha para serviços diferentes. E por fim, utilizar

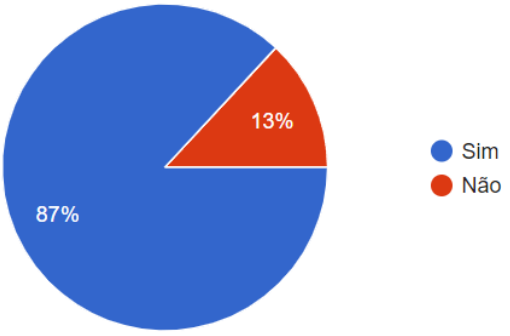
autenticação de dois fatores que foi introduzida recentemente para atender à demanda das organizações por fornecer opções de autenticação mais fortes para seus usuários, já que a autenticação de fator único, como senhas, não é mais considerada segura na internet (ALOUL; EL-HAJJ; ZAHIDI, 2009).

Resultados e Discussão

Em um eventual ataque MITM a uma rede pública onde é disponibilizado um *Wi-Fi* aberto, por exemplo, o invasor pode obter informações submetidas por uma possível vítima. Caso ela inicie uma sessão em algum serviço digital, o invasor terá acesso facilmente a esses dados, onde posteriormente, poderá utilizá-los para realizar novos ataques.

Deste modo, em uma pesquisa de campo realizada neste estudo verificamos que, com base na Figura 2, 87% das pessoas já efetuaram *login* em um serviço digital ou realizaram uma transferência bancária por meio de uma rede pública.

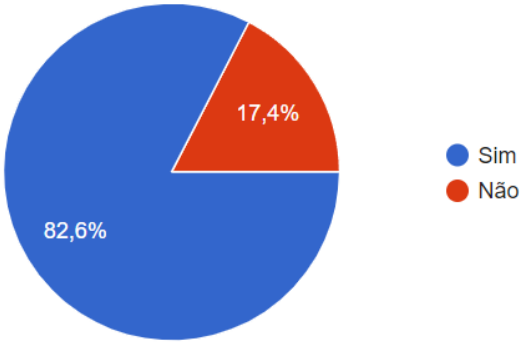
Figura 2: Resultados da questão a respeito de, efetuar *logins* ou transferências bancárias usando redes públicas



Fonte: Elaborado pelos autores (2022)

De acordo com a Figura 3, 82,6% das pessoas utilizam a mesma senha para serviços diferentes, sendo maléfico já que outras aplicações podem ser acessadas com a mesma informação.

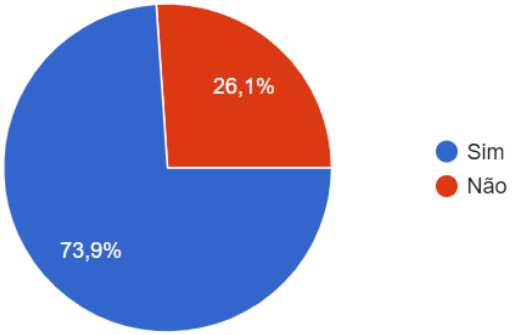
Figura 3: Resultados da questão sobre usar a mesma senha em serviços diferentes



Fonte: Elaborado pelos autores (2022)

Conforme mostrado na figura 4, 73,9% das pessoas utilizam autenticação de duas etapas, sendo positivo pois o usuário teria que permitir a conclusão de um novo acesso.

Figura 4: Resultados da questão quanto ao uso de autenticação de dois fatores em algum serviço digital



Fonte: Elaborado pelos autores (2022)

Conclusões

O momento atual é marcado não pelo diferencial, mas sim pela necessidade de algo estar *online*. Cada vez mais serviços essenciais já estão disponíveis com uma maior facilidade às pessoas, como por exemplo aplicativos de transações bancárias, comércio eletrônico e até mesmo aqueles que lidam com dados confidenciais, como informações de carreira e identidade. Assim concluímos que as pessoas não estão adequadamente seguras, devido a falta de informação e aptidão necessária para sua privacidade, já que suas informações estão cada vez mais voláteis.

Agradecimentos

Gostaríamos de agradecer ao professor Lucas de Araujo Oliveira por ter nos auxiliado e ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – campus Barretos, pela oportunidade oferecida aos alunos de obter tal experiência.

Referências Bibliográficas

OLIVEIRA, Ingrid. Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%. CNN Brasil [online], 19 ago. 2022. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/>. Acesso em: 28 set. 2022.

KAPLANIS, Charalampos. *Detection and prevention of Man in the Middle attacks in Wi-Fi technology*. Diss. Aalborg University, 2015.

CONTI, Mauro; DRAGONI, Nicola; LESYK, Viktor. *A survey of man in the middle attacks*. IEEE communications surveys & tutorials, 2016.

ATAQUE *man-in-the-middle* o que é?. Claranet, 2022. Disponível em: <https://br.claranet.com/blog/man-in-the-middle-o-que-e>. Acesso em: 28 set. 2022.

ALOUL, Fad; EL-HAJJ, Wassim; ZAHIDI, Syed. *Two factor authentication using mobile phones*. IEEE/ACS international conference on computer systems and applications. IEEE, 2009.