REDES PRIVADAS VIRTUAIS:

O USO DO OPENVPN COMO SOLUÇÃO DE VPN NA EMPRESA SUPPORT IT

Luiz Antonio De Oliveira Machado[1]
João Padilha Moreira[2]
Anderson Silva[3]
Marcelo Neves[4]
Jader Rodrigues[5]

RESUMO

Com o avanço da pandemia do Coronavírus, empresas como a Support It sentiram a necessidade de adaptar suas dinâmicas de trabalho às medidas de isolamento social recomendadas pelas autoridades, a fim de que houvesse a garantia da segurança e saúde (BRASIL, 2020). Com isso, os olhares voltaram-se para o trabalho remoto. Devido o aumento de ataques virtuais principalmente na ferramenta de acesso remoto RDP, este artigo baseia-se na possível solução de minimizar os ataques e garantir a segurança dos dados que trafegam da empresa até seus funcionários em *home office*, com segurança, através da internet, por meio de redes privadas virtuais VPN, o protocolo escolhido para realizar a comunicação VPN foi o OpenVPN.

ABSTRACT

With the advancement of the Coronavirus pandemic, companies such as Support it felt the need to adapt their work dynamics to social isolation measures by the authorities, in order to ensure safety and health (BRASIL, 2020). With that, the eyes turn to remote work. Advance the increase of virtual mainly in the tool of remote access RDP, this article is based on the possible solution to mitigate the attacks and to guarantee the security of the data that travels from the company to its employees in home office, safely, through the internet, for through VPN virtual private networks, the protocol chosen to carry out VPN communication for OpenVPN.

[1]Acadêmico do Curso Superior de Tecnologia em Sistemas para Internet - luiz.machado@alcidesmaya.edu.br
[2]Professor do Curso Superior de Tecnologia em Sistemas para Internet - joao_moreira@alcidesmaya.edu.br
[3]Professor do Curso Superior de Tecnologia em Redes de Computadores - anderson_silva@alcidesmaya.edu.br
[4]Professor do Curso Superior de Tecnologia em Redes de Computadores - marcelo_neves@alcidesmaya.edu.br
[5]Professor do Curso Superior de Tecnologia em Redes de Computadores - jader_rodrigues@alcidesmaya.edu.br

INTRODUÇÃO

Com o crescente aumento dos casos de infecção pelo coronavírus (COVID-19), empresas de todos os segmentos precisam adaptar suas dinâmicas de trabalho às medidas de isolamento social recomendadas pelas autoridades, a fim de que houvesse a garantia da segurança e saúde (BRASIL, 2020). Com isso, os olhares voltaram-se para o trabalho remoto. Com a empresa do estudo de caso desta pesquisa, Support It, não foi diferente.

De acordo com o ministério da saúde a Covid-19 é uma infecção respiratória aguda causada pelo coronavírus SARS-CoV-2, potencialmente grave, de elevada transmissibilidade e de distribuição global (BRASIL, 2020). No Brasil, o primeiro caso confirmado foi em 26 de fevereiro, em São Paulo. No mesmo mês, começaram as primeiras ações governamentais ligadas à pandemia da COVID-19, com a repatriação dos brasileiros que viviam em Wuhan, cidade chinesa epicentro da infecção. Desde então, a pandemia e as ações governamentais foram variadas, com reduções e aumentos no número de casos, medidas como lockdown e também o início da vacinação em algumas localidades (SANAR, 2020).

Conforme a definição proposta pela Organização Internacional do Trabalho (OIT), o *home office* pode ser definido como o modo de exercer atividades em espaços diferentes do ambiente empresarial (QUEIROGA, 2020). Os profissionais se mantêm conectados através de tecnologias que viabilizam as conexões remotas, tais como, a VPN. Como bem nos assegura a Sociedade Brasileira de Teletrabalho e Teleatividades (SOBRATT), o home office ou teletrabalho assim se define:

> O teletrabalho pode ser definido como uma espécie do gênero trabalho à distância, no qual a prestação de serviços pelo empregado se dá preponderantemente fora da sede da empresa, por meio da utilização de computadores e outros meios eletrônicos de comunicação. (SOBRATT, 2019).

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

Posto isso, o modo de conexão externa ao ambiente corporativo da Support It é feito através do *Remote Desktop Protocol* (RDP), protocolo que permite que um usuário se conecte a um computador, rodando o *Microsoft Terminal Services*. Porém, este modo não é eficiente em termos de segurança. Segundo Fracassi (2019), as vulnerabilidades do RDP ocorrem quando a porta 3389 está exposta para internet e com isso o servidor está sujeito à ataques como o de força bruta onde invasor tenta, de maneira automática e incansável, várias combinações de senha até que a solução correta é encontrada.

Surgiu, então, a necessidade de se criar uma solução que possibilitasse que os funcionários da *Support IT* acessassem serviços como pastas, telefonia e sistemas de gerenciamento interno, remotamente, porém de forma segura e estável, tanto para a empresa quanto para o empregado.

Para atender à necessidade, uma rede privada virtual foi projetada a fim de disponibilizar o acesso remoto aos servidores da Support It. A ferramenta utilizada foi o *OpenVPN* integrado ao *firewall Pfsense Freebsd*. O *OpenVPN* utiliza um túnel criptografado para garantir que as informações sejam transmitidas de forma segura. Dessa forma, o intuito desta pesquisa é reunir informações com o propósito de responder a questão central: de que maneira o OpenVPN pode contribuir para a transferência de dados da empresa até seus funcionários em *home office*, com segurança, através da internet?

Palavras-chave: SARS-CoV-2, *home office,* lockdown, VPN, OpenVPN, RDP.

MOTIVAÇÃO

Considerando o cenário mundial de pandemia, Camargo (2020) salienta que 80% dos gestores aprovaram o modelo *home office*, no início de 2020. Com isso, os ataques usando as vulnerabilidades do RDP e TS aumentaram 330%, conforme informa Rodrigues (2020), o que indica que a proteção é necessária com urgência nesta situação.

Devido a necessidade de garantir a privacidade e segurança dos dados que trafegam da empresa até seus funcionários em *home office*, esse artigo se justifica através do estudo de como a solução *OpenVPN* pode contribuir para o aumento de segurança em conexões remotas. Em colaboração com o seu público alvo, a proposta de contribuir com o desenvolvimento de redes mais seguras.

SUPPORT IT EM TEMPOS DE PANDEMIA

Localizada em Cachoeirinha-RS a Support It é uma empresa de tecnologia da informação, que atua nos pilares de segurança da informação, virtualização e tecnologia Volp. Assim como as grandes empresas, precisou adaptar sua logística de trabalho ao contexto local e mundial, priorizando a saúde e bem estar dos funcionários direcionando toda sua operação para o home office.

Devido aos decretos propostos pelos governantes (BRASIL, 2020), a Support It migrou toda sua operação para o home office, com isso surgiram as dúvidas quanto a segurança da informação, e iniciou-se uma pesquisa para mitigar as vulnerabilidades dos acessos remotos realizados pelos funcionários aos servidores da Support It, inicialmente o acesso estava sendo feito através da ferramenta *remote Desktop protocol (RDP),* da Microsoft, entretanto as pesquisas realizadas evidenciaram que as tentativas de invasão a este tipo de serviço chegaram 330%. A fim de minimizar as tentativas de invasão e evitar possíveis perdas de dados e indisponibilidade dos servidores, uma rede segura foi projetada para garantir a integridade das informações.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

O protocolo utilizado na empresa para preservar a integridade dos dados transpassados via conexão remota, foi o protocolo de VPN, OpenVPN, que tem por objetivo criptografar o caminho de origem e destino dos dados através de um túnel virtual.

PROTOCOLO RDP

A sigla do RDP significa *Remote Desktop Protocol,* quer dizer Protocolo de Área de trabalho Remota, este protocolo permite que usuários conectem em suas estações de trabalho sem que seja necessário estar fisicamente próximo a seus computadores.(BARBOSA, 2020)

Este protocolo desenvolvido pela Microsoft é muito utilizado por quem trabalha à distância, contribui para mobilidade da empresa viabilizando o acesso remoto através da ferramenta *Remote Desktop Connection,* entretanto para que os acessos sejam concebidos é necessário que o administrador da rede permite as conexões remotas externas abrindo a porta lógica de acesso ao *RDP,* a 3389.

Embora esse protocolo seja um facilitador de acesso para as empresas ainda mais neste período de pandemia, ele possui vulnerabilidade que estão sendo exploradas por invasores, de acordo com a pesquisa realizada pela empresa Kaspersky, com a adesão em massa das empresas ao home office o índice de tentativas de invasão no protocolo RDP teve um aumento de mais de 300%.

ATAQUE DE FORÇA BRUTA

Segundo Albors (2020) o ataque de força bruta ocorre quando o invasor usa maneiras de testar diversas combinações de senha a fim de acessar o computador da vítima. A principal funcionalidade do ataque de força bruta é tentar através de tentativa e erro decodificar a senha do alvo desejado, por isso sugere-se sempre usar senhas mais complexas para dificultar o sucesso da invasão.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

RANSOMWARE

De acordo com a ESET (2018) o ransomware é uma espécie de malware (Software mal-intencionado) que os criminosos instalam em computadores, sem consentimento da vítima. O ransomware possibilita aos criminosos virtuais bloquear ou criptografar os dados dos computadores de forma remota e solicitam valores, geralmente em bitcoin, para que os dados possam ser resgatados.

Os modos mais comuns de um usuário ser atacado por ransomware é através de falsas mensagens de e-mails ou de página web, ataque de força bruta ou através

Falsas alegações sobre conteúdo ilegal como por exemplo, a pirataria de software. (COSSETTI, 2019)

> Perigoso para você e altamente lucrativo para cibercriminosos, o ransomware assumiu o primeiro lugar na lista de ameaças de segurança. As tentativas de ataque e infecção aumentaram muito nos últimos anos e continuarão a aumentar, pois cada versão parece ficar mais poderosa e mais destrutiva. (MATEIU, 2018)

A SOLUÇÃO

Como vimos, os ataques de força bruta estão aumentando, assim como o ransomware e para minimizar o impacto de uma suposta invasão e perda dos dados a Support It criou uma rede privada virtual (VPN) para garantir a segurança e privacidade dos dados que trafegam entre o ambiente home office e o corporativo.

De acordo com Roveda (2020) VPN é a sigla de abreviação de *Virtual Private Network,*que tem como característica estabelecer um túnel virtual criptografado para que os dados trafeguem de forma segura.

O protocolo de VPN utilizado pela a empresa foi o *OpenVPN,* segundo Mocan (2021) O *OpenVPN* é tanto um protocolo de VPN de código aberto quanto um programa VPN que permite às pessoas rodar conexões VPN seguras. A maioria das VPNs oferece esse protocolo porque é muito seguro (ele utiliza a biblioteca OpenSSL e a criptografia 256 bits) e funciona em várias plataformas. O *OpenVPN* é considerado a melhor escolha entre os protocolos de VPN.

> Essencialmente, uma VPN serve para impedir que o usuário seja identificado na internet. Ao se conectar em uma rede privada, este recebe um número de IP aleatório, que difere do seu próprio, e todos os seus dados de navegação, mesmo os mais banais, são totalmente criptografados, barrando operadoras de internet, governos e hackers. (GOGONI, 2019)

Visto isso, é possível afirmar que o *OpenVPN* é um modo seguro de garantir a comunicação dos clientes ao datacenter da empresa Support It.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

REFERÊNCIAS:

ALBORS, Josep. **Saiba o que é um ataque de força bruta e como funciona**. 2020. Disponível em: https://www.welivesecurity.com/br/2020/06/26/o-que-e-um-ataque-de-forca-bruta/. Acesso em: 14 maio 2021.

BARBOSA, Daniel Cunha. **O que é um RDP e para que serve?** 2020. Disponível em: https://www.welivesecurity.com/br/2020/06/30/o-que-e-um-rdp-e-para-que-serve/#:~:text=A%20sigla%20RDP%20vem%20do,fisicamente%20pr%C3%B3ximo%20a%20seus%20computadores.. Acesso em: 14 maio 2021.

BRASIL. MINISTÉRIO DA SAÚDE. (org.). **CORONAVÍRUS (COVID-19)**: sobre a doença. Sobre a doença. 2020. Disponível em: https://coronavirus.saude.gov.br/sobre-a-doenca#o-que-e-covid. Acesso em: 04 maio 2020.

CAMARGO, Renato. **Novidade, trabalho remoto agradou a 80% dos gestores brasileiros**. 2020. Disponível em: https://noticias.r7.com/economia/correcao-novidade-trabalho-remoto-agradou-a-80-dos-gestores-brasileiros-22052020. Acesso em: 12 mar. 2021.

COSSETTI, Melissa Cruz. **O que é um ransomware?** 2019. Disponível em: https://tecnoblog.net/275356/o-que-e-um-ransomware/. Acesso em: 14 maio 2021.

ESET ENJOY SAFER TECHNOLOGY. **Ransomware**. 2019. Disponível em: https://www.eset.com/br/ransomware/. Acesso em: 14 maio 2021

FRACASSI, João Batista. **Conheça as falhas no protocolo RDP da Microsoft**: conheça as vulnerabilidades conhecidas do rdp (remote desktop protocol) e entenda como sua máquina pode ficar vulnerável contra hackers e ataques direcionados. 2019. Disponível em: https://www.interop.com.br/blog/rdp/. Acesso em: 02 mar. 2021.

GOGONI, Ronaldo. **O que é VPN?** 2019. Disponível em: https://tecnoblog.net/283693/o-que-e-vpn/. Acesso em: 14 maio 2021.

MATEIU, Monica. **O guia definitivo para ransomware**. 2018. Disponível em: https://www.avg.com/pt/signal/what-is-ransomware. Acesso em: 14 maio 2021.

MOCAN, Tim. **O que é o OpenVPN e como funciona?** 2021. Disponível em: https://www.cactusvpn.com/pt/guia-iniciantes-vpn/o-que-e-o-openvpn/. Acesso em: 14 maio 2021.

QUEIROGA, Fabiana. **O trabalho e as medidas de contenção da COVID-19**: orientações para o home office durante a pandemia da covid-19. Orientações para o home office durante a pandemia da COVID-19. 2020. Disponível em: https://play.google.com/books/reader?id=XuPuDwAAQBAJ&hl=pt-BR&lr=lang_pt&printsec=frontcover&pg=GBS.PA2. Acesso em: 06 mar. 2021.

RODRIGUES, Renato. **Ataques usando acesso remoto crescem 330% no Brasil**: número de ataques diários de força bruta à ferramenta rdp passou de 402 mil no início de fevereiro para 1,7 milhão em abril. 2020. Disponível em: https://www.kaspersky.com.br/blog/ataques-rdp-brasil-home-office-pesquisa/15590/. Acesso em: 10 fev. 2021

ROVEDA, Ugo. **VPN: o que é, como funciona, por que e quando usar VPN?** 2020. Disponível em: https://kenzie.com.br/blog/vpn/. Acesso em: 14 maio 2021.

SANAR (Brasil). **Coronavírus**: linha do tempo do coronavírus no brasil. Linha do tempo do Coronavírus no Brasil. 2020. Disponível em: https://www.sanarmed.com/linha-do-tempo-do-coronavirus-no-brasil. Acesso em: 03 mar. 2021.

TELEATIVIDADES, Sociedade Brasileira de Teletrabalho e. **O teletrabalho e a responsabilidade do empregador em casos de acidente de trabalho**: conceito e legislação aplicável. Conceito e legislação aplicável. 2019. Disponível em: http://www.sobratt.org.br/index.php/07052019-o-teletrabalho-e-a-responsabilidade-do-empregador-em-casos-de-acidente-de-trabalho/#:~:text=Neste%20contexto%2C%20o%20teletrabalho%20pode,outros%20meios%20eletr%C3%B4nicos%20de%20comunica%C3%A7%C3%A3o.. Acesso em: 04 maio 2021.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.