SEGURANÇA NA ERA DOS DADOS: UMA REVISÃO SOBRE A IMPORTÂNCIA E APLICAÇÕES DAS VPNs

SECURITY IN THE AGE OF DATA: A REVIEW ON THE IMPORTANCE AND APPLICATIONS OF VPNs

Leonardo Fava Calcanho, aluno do Curso Superior de Tecnologia em Segurança da Informação na FATEC "Ministro Ralph Biasi" Americana, leonardo.calcanho@fatec.sp.gov.br
Orientador: Prof. Maxwel Vitorino Da Silva, maxwel.silva5@fatec.sp.gov.br

Resumo

Este artigo tem o intuito de explicar e estudar o que é a *Virtual Private Network* (VPN), listar as vantagens de seu uso, descrever sua importância atualmente, considerando o uso amplificado da computadores e celulares e de seu uso para o armazenamento de dados pessoais sigilosos, como os dados bancários. Além disso, buscou-se verificar as falhas da VPN apresentando suas aplicações em diversos ramos, para isso, realizou-se pesquisa bibliográfica em livros, artigos, sites, periódicos e simpósios. Ao final, conclui-se que a VPN tem grande importância na segurança dos dados, sobretudo em redes públicas, as quais possíveis invasores têm um acesso facilitado. Com isso, o artigo cumpre seu objetivo em mostrar o estudo e a apresentação dessa tecnologia para a sociedade geral.

Palavras-chave: Segurança da Informação, *Virtual Private Network*, segurança de dados.

Abstract

This article aims to explain and study what Virtual Private Network (VPN) is, list the advantages of its use, describe its importance today, considering the amplified use of computers and cell phones and their use for storing data. sensitive personal data, such as bank details. In addition, we sought to verify the VPN failures by presenting its applications in various fields, for this, bibliographic research was carried out in books, articles, websites, periodicals, and symposia. In the end, it is concluded that VPN has great importance in data security, especially in public networks, to which possible intruders have easy access. With this, the article fulfills its objective of showing the study and presentation of this technology to society in general.

Keywords*: Information Security, Virtual Private Network, data security.*

1. Introdução

Atualmente observa-se em nossa sociedade a transição do modelo de trabalho e negócios do formato presencial para o formato *online* ou de *home-office*. No entanto, há riscos envolvidos nessa transição, incluindo a quebra de sigilo dos dados. Uma vez que, esses dados são violados, comprometem a sua confidencialidade e integridade.

E disso surge a necessidade de as organizações utilizar uma tecnologia conhecida coma VPN (do inglês, *Virtual Private Network*), o qual foi criado para permitir que as empresas tivessem conexões de rede seguras e protegidas.

De acordo com Ezra et al. (2021), as VPNs são empregadas em diversos ramos, desde microempresas até grandes multinacionais, em colégios, universidade e governos. É graças a esse sistema que os dados e as informações podem manter-se seguras com seus proprietários, o uso dessa tecnologia vai conforme o esforço global em manter os dados e informações pessoais seguras, um dos exemplos dessa cooperação nacional e mundial é a sanção da Lei Geral de Proteção de Dados (13.709/2018).

Com base nessa motivação, o presente artigo busca investigar a história das VPNs, seu funcionamento, a sua importância e aplicações em empresas e instituições. Dessa forma, a pesquisa foi realizada com base em uma revisão das literaturas e referências disponíveis a fim de garantir o estudo e a apresentação dessa tecnologia para a sociedade geral.

2. Referencial Teórico

Segundo o artigo "*Secured Communication Using Virtual Private Network* (VPN)" (Ezra et al., 2021), a evolução e a era dos programas e serviços mais recentes, juntamente com a ampliação das comunicações criptografadas, dificultam os visitantes do site em uma empresa de segurança.

De acordo com Ezra, as redes privadas virtuais (VPNs) são instâncias de provedor de comunicação criptografada que estão se tornando cada vez mais utilizadas, como forma de contornar a censura, além de obter acesso a ofertas geograficamente bloqueadas, e é nestes principais autores que o artigo baseia-se.

3. Metodologia

Esse artigo trata-se de um estudo a respeito das VPNs, Virtual Private Network, como já dito. Para ser bem-sucedido, a investigação toda se baseia em dados colhidos em um compilado de fontes teóricas em livros, monografias, outros artigos, simpósios, periódicos e teses, ou seja, trata-se de uma pesquisa bibliográfica onde explorou-se outros autores, dados e informações a fim de que este artigo atinja seu objetivo.

4. Resultados e Discussões

4.1. O que é VPN?

Com o avanço das tecnologias e a necessidade frequente de estar conectado, muitas pessoas têm acesso à rede pública, o que é arriscado, pois pode levar a que intrusos acedam a dados confidenciais. É nesse cenário que a VPN se insere, ele estabelece uma conexão protegida quando se está em uma rede pública, criptografando o tráfego de Internet e disfarçando sua identidade online, para que terceiros não podem entendê-la, tornando mais difícil para terceiros roubar e rastrear seus dados.

Além disso, a tecnologia VPN pode ajudar os usuários a contornar a censura, contornar blocos de conteúdo e desbloquear restrições do site, facilitando a obtenção de informações através da Internet. Alguns sites são permanentemente restringidos de serem acessados dentro de uma determinada região, e quando um indivíduo fora dessa região tenta acessá-los, eles são bloqueados.

No entanto, como a VPN esconde um endereço IP e a localização física porque pode encriptar o tráfego da Internet e permite acessar facilmente a esses sites (Teymourlouei & Harris, 2019). Isso ajuda a evitar que as pessoas espiem o que você está fazendo na Internet. Portanto, a VPN é virtual porque cria um túnel digital, já que nenhuma conexão física conecta os usuários aos servidores VPN. Também é privada porque encripta os dados dos utilizadores escondendo o seu endereço IP, e é uma rede uma vez que cria uma ligação entre vários dispositivos.

Assim, os seus serviços primários são encriptar a ligação à Internet dos utilizadores, proteger os seus dados na rede pública e permitir-lhes o acesso a blocos de conteúdo baseados em localização. Além disso, os usuários podem acessar sites bloqueados, evitar o rastreamento

de ISPs e evitar a censura da Internet.

As conexões VPN são criadas por roteadores, mas, os clientes devem entender que diferentes roteadores estabelecem essas conexões e saber qual é a melhor para eles. Há um roteador de consumo que suporta conexões VPN e um roteador empresarial que é mais dinâmico e oferece todas as medidas de segurança difíceis para os intrusos penetrarem e violarem os dados (Ezra et al., 2021).

A configuração de uma VPN é simples e confiável para pessoas e organizações que desejam enviar informações para outras localizações geográficas através de uma conexão segura com a Internet. Porém, encontrar o tamanho apropriado do roteador que estabelece a rede VPN depende de muitos fatores, incluindo o tamanho da organização.

Suponha que se esteja operando uma empresa de pequeno a médio porte. Nesse caso, um roteador VPN é ideal, pois permite o túnel VPN entre as redes, permitindo a comunicação de entrada e saída.

4.2. História das VPNs

Quando a tecnologia evoluiu e o uso da internet se tornou desenfreado, houve inúmeros movimentos para proteger e criptografar dados. Antes da inovação da VPN, as tecnologias iniciais eram usadas para criptografar dados, como a ARPANET, que era baseada em uma rede de comutação de pacotes que levou ao desenvolvimento do *Transfer Control Protocol/Internet Protocol* (Beutler, 2021).

A partir daí, foi quando a VPN começou a ser implementada. Isto foi motivado pela utilização diária da Internet, que aumentou rapidamente à medida que muitas pessoas foram agora expostas a atividades online. Isto fez com que as pessoas começassem a ver a necessidade de proteger os seus sistemas contra-ataques de vírus e malware. Mesmo assim, eles também exigiam um software que pudesse ajudar a esconder suas quatro atividades online, como o histórico de navegação.

Assim, a VPN começou a ser praticado no início dos anos 2000, mas era tipicamente empregado para o uso empresarial (Beutler, 2021). Após a série de violações de segurança de alto perfil, particularmente a que aconteceu em 2010, muitos consumidores começaram a ver a

importância das VPNs.

As VPNs têm vindo a avançar para garantir que oferecem medidas de segurança que satisfazem e excedem as exigências do mercado. A VPN atual é a mais segura e confiável para permitir aos utilizadores o acesso a conteúdo restrito.

4.3. VPNs são seguras de se usar

A principal função das VPNs é proteger a atividade online do utilizador, e por isso são muito seguras. Elas funcionam encriptando a ligação à Internet do utilizador, encriptando todo o seu tráfego online e encaminhando-o através de uma ligação ponto a ponto, estabelecendo assim uma rede privada na rede pública (Teymourlouei & Harris, 2019).

Isto é ideal, pois ninguém irá interceptar seu tráfego de dados mesmo enquanto estiver usando a rede pública, oferecendo uma série de benefícios de segurança, privacidade e desempenho. Além de proteger seus dados contra intrusos, ele também esconde sua localização, ocultando o endereço IP exato do seu sistema. Isso torna difícil ser rastreado por qualquer pessoa que possa estar bisbilhotando em sua rede local.

Além disso, oferece uma transferência de dados segura que é ideal quando se faz negócios sensíveis como a banca online pela Internet. Qualquer mensagem pessoal enviada através da Internet é protegida e não pode ser acessada pelo homem em um ataque intermediário porque a VPN criptografa a comunicação com seu servidor (Ezra et al., 2021).

Isto é importante mesmo para o indivíduo que gosta de aceder gratuitamente ao Wi-Fi público. Qualquer pessoa pode aceder ao seu dispositivo sem uma VPN em Wi-Fi público, comprometendo os seus dados ou roubando informações valiosas.

Portanto, VPN é uma necessidade básica que qualquer pessoa que conduz os seus negócios online muitas vezes precisará de ter. Poupará nos recursos que poderiam ser utilizados para reter os dados que foram violados e ajudará a preservar a confidencialidade online.

4.4. Importância das VPNs

As VPNs têm níveis básicos e avançados de usabilidade. A um nível básico, espera-se que a sua privacidade seja salvaguardada uma vez que a VPN ajuda a mascarar o endereço IP,

localização, histórico de pesquisas e entre outros dados pessoais.

Isto permitirá evitar que sejam rastreados a partir do site pelo qual passam muito tempo navegando, navegadores e provedores de serviços de Internet, entre outros intrusos que possam ter acesso aos seus dados (Teymourlouei & Harris, 2019).

Também, a um nível básico, espera-se segurança protegendo suas informações pessoais e outros dados que possam estar em trânsito. Além destes níveis básicos de proteção, a VPN poderia ser configurada para fornecer uma rede avançada e mais segura. Por exemplo, todos podem aceder ao seu celular utilizando websites e aplicativos.

No entanto, a maioria das pessoas desconhece que estes aplicativos e sites podem rastrear suas atividades através da análise dos dados que coletam. Com a ajuda de uma VPN, pode-se evitar que isso aconteça, uma vez que isso impedirá que este browser e outras aplicações acedam à ligação a que está ligado. A VPN também mantém a informação em trânsito segura e anônima.

Ao utilizar uma VPN avançada, pode-se obter uma encriptação de nível militar de 256 bits, implicando que os seus dados estejam mais seguros. Além disso, a VPN vai ajudar a escapar ao estrangulamento dos dados, que acontece quando o usuário consumiu uma certa quantidade de dados e o ISP diminuiu a velocidade dos seus serviços.

Quando isto acontece, o ISP pode facilmente monitorizar as suas atividades online, e qualquer intruso pode ter acesso a elas. No entanto, se alguém estiver usando uma VPN, eles não podem ser afetados, pois não haverá limite de dados.

O limite de dados é usado principalmente pelo ISP quando eles querem maximizar a velocidade da Internet dos seus utilizadores; no entanto, permite-lhes monitorizar todas as suas atividades na Internet (Raj & Srinivasulu, 2022).

A utilização de uma VPN permite-lhes evitar o estrangulamento da largura de banda, que vem com a velocidade lenta da Internet quando acedem a certos sites e em alturas diferentes. Na maioria dos casos, isto acontece devido ao problema com os controles administrativos ou com o ISP, o que implica que podem estar a monitorizar as suas atividades.

Uma VPN, portanto, ajudará a evitar isso, porque funciona para combater a lentidão, encriptando o tráfego de Internet do dispositivo, impedindo que outros na mesma rede leiam o

seu conteúdo de tráfego online, e escondendo o destino.

Outro fator crítico é o acesso a serviços bloqueados por região, uma vez que funciona alterando o endereço IP do usuário. Isto fará com que o provedor de conteúdo pense que você está a partir da sua localização ou região de acesso. No entanto, isto não é ético e não é defendido, mas é ideal durante investigações ou quando se faz trabalho de pesquisa.

Antes de empregar, é aconselhável verificar os termos do contrato de serviço para encontrar o que é permitido pelos serviços que você quer acessar e garantir que você esteja ciente das penalidades que vêm com o uso de uma VPN para contornar essa regra (Aswad & Sonic, 2020).

Outro fator importante para os turistas e para aqueles que viajam frequentemente é que isso pode ajudá-los a evitar a censura. Alguns países proíbem o acesso a certos websites e plataformas de redes sociais. No entanto, através de uma VPN, pode-se aceder facilmente a eles, uma vez que isso fará com que o seu tráfego pareça vir daquela região do seu fornecimento.

As linhas de ligação empresarial são relativamente caras, mas uma VPN dá à empresa opções de linhas alugadas mais baratas. O uso de uma VPN permite que a empresa conecte seus muitos locais de escritório sem ter que pagar por linhas de capacidade de rede caras (Aswad & Sonic, 2020).

Eles podem conectar-se a redes públicas usanda VPN sobre linhas alugadas locais menos dispendiosas, poupando-lhes muito dinheiro. Além disso, a VPN pode ajudá-lo a poupar dinheiro ligando-se ao seu ponto de acesso ISP local, em vez de se ligar através de servidores de acesso remoto e redes discadas enquanto converte longas distâncias.

Além disso, o roteador VPN poderia ser configurado para funcionar como cliente e servidor, indicando a sua dinâmica de usabilidade. Então, se a organização tiver especialistas em TI, eles podem executar o software DD-WRT de código aberto, que substituirá o sistema operacional do roteador para fornecer recursos adicionais de segurança. Além disso, muitos roteadores VPN avançados suportam conexões de rede de área ampla (WAN) (Aswad & Sonuc, 2020).

Isto foi personalizado para fazer balanceamento de carga e failover e incorporado com outros recursos de segurança para garantir que um esteja operando em uma conexão segura.

Quando se obtém um roteador VPN mais avançado, pode-se obter até 45 túneis com excelentes firewalls que suportam a filtragem de tráfegos de entrada e saída.

Ele também pode realizar filtragem de conteúdo e impor níveis mínimos de complexidade para senha e chaves de criptografia para garantir que o negócio opere em um túnel seguro. Isso facilita a comunicação entre duas localizações geográficas sem encontrar um ataque de homem no meio.

4.5. Falhas nas VPNs

Mesmo que os benefícios de uma VPN superem os seus inconvenientes, alguns desafios potenciais podem ocorrer.

O roteador VPN de consumo suporta a passagem da VPN?

A resposta a essa pergunta é delicada para as empresas porque implica que se alguém tem software VPN nos seus sistemas, pode permitir a passagem do túnel para a Internet. Além disso, a VPN funciona encriptando a ligação do utilizador, isto pode atrasar a ligação reduzindo a velocidade da ligação à Internet (Wei et al., 2022).

Algumas tarefas requerem alta conectividade com a Internet, tornando-as difíceis de serem realizadas. As VPNs são confiáveis e eficientes, entretanto, são ilegais em alguns países, e os países decretaram políticas pesadas sobre sua usabilidade, com aqueles que violam essa regra sendo fortemente penalizados. Isto torna mais difícil para as pessoas utilizarem as suas capacidades, por isso os estrangeiros estão em digressão por esse país.

Portanto, é aconselhável verificar a legislação desse país antes de utilizar a VPN. Muitos dos negócios são geridos por especialistas não especialistas em TI. Faltam-lhes conhecimentos e competências sobre a funcionalidade da VPN, o que dificulta a sua instalação ou até mesmo a sua cautela em relação à sua importância no negócio.

Isto torna difícil para eles distinguir a VPN apropriada para o seu negócio, já que são de duas categorias: consumidor e negócio. Se eles empregam a empresa, é relativamente complicado, tornando difícil a sua instalação (Cui et al., 2020).

Além disso, eles podem não ter conhecimentos especializados para encriptar o túnel

VPN, pois é difícil representar a qualidade de encriptação da VPN.

4.6. Empresas que utilizam VPNs

As VPNs são imprescindíveis para as empresas que conduzem as suas atividades de forma online. Uma vez que, dificultará eventuais violações de dados e evitar que seu sistema seja comprometido com mais frequência.

Porém, a maioria das organizações falhou em distinguir os roteadores adequados à sua usabilidade. Além disso, uma organização precisa entender sua lógica para uma VPN específica, resumindo-se a ter uma funcionalidade que suporte suas necessidades comerciais (Cui et al., 2020).

Algumas empresas requerem maior segurança do que possam perceber, muitas vezes motivadas pela necessidade de cumprir com as restrições regulatórias. Além disso, uma VPN apropriada precisa de múltiplas redes sem fio para permitir que os clientes acessem a largura de banda Wi-Fi da organização sem comprometer a rede de produção de nossiness.

Sendo assim, o roteador VPN usado para estabelecer a conexão deve conseguir suportar muitos usuários na rede sem fio e lidar com muitos túneis VPN. Portanto, numerosas empresas usam VPNs, entretanto, o foco será mais na organização que fabrica a VPN porque usam a sua VPN para assegurar a sua comunicação de dados.

A Aura, uma organização americana, lançou o seu primeiro serviça VPN em 2008. A organização é proprietária de hotspot shield, VPN touch, Veepee VPN, VPN 360, e Hexatech.

Além disso, uma organização j2 global está envolvida com um sistema de rede VPN (Kasunic, 2022), eles conduzem toda a sua comunicação através da Internet através de um túnel VPN seguro.

Entre outras empresas estão Actmobile Networks, Kape Technologies, Gaditek e Avast. Contudo, para indicar a popularidade das tecnologias VPN nas empresas, uma vez que essas tecnologias são muito eficazes e confiáveis quando transmitem informações em diferentes localizações geográficas.

5. Considerações Finais

Apresentou-se nesse artigo, as VPNs que são tecnologias quase que imprescindíveis, uma vez que elas são confiáveis e eficientes quando bem configuradas, uma vez que o conceito é de assegurar o estabelecimento de um túnel seguro para a transmissão de dados. De acordo com (Kasunic, 2022) muitas empresas declararam que a sua taxa de violação de dados caiu drasticamente após incorporar VPNs na sua rede.

Isto permitiu-lhes aceder a conteúdos bloqueados que não podem ser transmitidos a partir de alguma localização geográfica. Portanto, para indivíduos, organizações corporativas ou instituições que procuram formas seguras de transmitir os seus dados, a VPN é a solução final.

Referências

ASWAD, S., & SONUC, E. (2020). Classification of VPN Network Traffic Flow Using Time Related Features on Apache Spark. 2020 4Th International Symposium On Multidisciplinary Studies And Innovative Technologies (ISMSIT). Disponível em: https://doi.org/10.1109/ismsit50672.2020.9254893

BEUTLER, M. (2021). Virtual Private Networks as Digital Infrastructure. ArcGIS StoryMaps. Disponível em: https://storymaps.arcgis.com/stories/bea5c5118cb0458d8bb8c3c0f2aaf467.

CUI, P., YANG, R., & DING, Z. (2020). Detect and analyze the concurrent flaws of the BPEL process in a VPN-based approach. International Journal Of Services Technology And Management, 26(2/3), 182. Disponível em: https://doi.org/10.1504/ijstm.2020.106745

EZRA, P., MISRA, S., AGRAWAL, A., OLURANTI, J., MASKELIUNAS, R., & DAMASEVICIUS, R. (2021). Secured Communication Using Virtual Private Network (VPN). Lecture Notes On Data Engineering And Communications Technologies, 309-319. Disponível em: https://doi.org/10.1007/978-981-16-3961-6_27

KASUNIC, K. (2022). These 7 Companies Secretly Own Dozens of VPNs. vpnMentor. Disponível em: https://www.vpnmentor.com/blog/companies-secretly-own-dozens-vpns/.

RAJ, J., & SRINIVASULU, S. (2022). Design of IoT Based VPN Gateway for Home Network. 2022 International Conference On Electronics And Renewable Systems (ICEARS). Disponível em: https://doi.org/10.1109/icears53579.2022.9751838

TEYMOURLOUEI, H., & HARRIS, V. (2019). Effective Methods to Monitor IT Infrastructure Security for Small Business. 2019 International Conference On Computational Science And Computational Intelligence (CSCI). Disponível em: https://doi.org/10.1109/csci49370.2019.00009

WEI, X., MIAO, W., ZENG, Z., WANG, Y., ZHAO, H., & HE, Y. ET AL. (2022). Research on Using Dynamic Thread Pool to Improve the Performance of VPN Gateway. 2022 7Th International Conference On Computer And Communication Systems (ICCCS). Disponível em: https://doi.org/10.1109/icccs55155.2022.9846591

Agradecimentos

Agradeço à minha família pelo apoio, ao meu professor orientador Prof. Maxwel Vitorino Da Silva a todos os servidores e professores da FATEC “Ministro Ralph Biasi” Americana.