CENTRO UNIVERSITÁRIO DE ANÁPOLIS – UniEVANGÉLICA
BACHARELADO EM ENGENHARIA DE SOFTWARE

ANDRÉ LUIS DA SILVA
JOÃO VICTOR DA SILVA

AMBIENTES SEGUROS PARA TRABALHAR HOME OFFICE

ANÁPOLIS
2021-01

ANDRÉ LUIS DA SILVA
JOÃO VICTOR DA SILVA

AMBIENTES SEGUROS PARA TRABALHAR HOME OFFICE

Trabalho de Conclusão de Curso I apresentado como requisito parcial para a conclusão da disciplina de Trabalho de Conclusão de Curso I do curso de Bacharelado em Engenharia de Software do Centro Universitário de Anápolis – UniEVANGÉLICA.

Orientador(a): Prof. Millys Fabrielle Araujo Carvalhaes.

ANÁPOLIS
2021-01

ANDRÉ LUIS DA SILVA
JOÃO VICTOR DA SILVA

AMBIENTES SEGUROS PARA TRABALHAR HOME OFFICE

Trabalho de Conclusão de Curso I apresentado como requisito parcial para a obtenção de grau do curso de Bacharelado em Engenharia de Software do Centro Universitário de Anápolis – UniEVANGÉLICA.

Aprovado(a) pela banca examinadora em [dia] de [mês] de 2021, composta por:

_____
Prof. [nome do professor]
Orientador

_____
Prof. [nome do professor]

_____
Prof. [nome do professor]

Resumo

Com a chegada da pandemia do novo coronavírus, obrigou muitas empresas e funcionários a trabalharem por meio de trabalho *home office*, isso fez com que o numero de casos de ataques hacker e vazamentos de dados aumentassem. O objetivo central do trabalho é implementar tecnologias que favorecem a segurança da informação em ambientes *home office*. Propõe-se, assim, a simulação de um ambiente de trabalho remoto realizando teste com as tecnologias atuais que promovem a segurança da informação e criar um manual de uso acordo com os resultados obtidos. Sob essa visão, *o home office* pode ter uma melhor imagem para empresas e funcionários que estão inseguros em utilizá-lo.

Palavras-chave*: Home Office*; Segurança da Informação; Hacker;

Sumário

1. Problema

Com a chegada da pandemia do novo coronavírus, muitas empresas foram obrigadas a se adaptar a um novo meio de trabalho: o *Home Office*. Este é um meio de um profissional trabalhar à distância, no qual se utiliza de equipamentos tecnológicos, como computadores, smartphones, tablets, entre outros (SOBRATT, [s.d.]).

O *Home Office* trouxe, também, ganhos na otimização de tempo para aqueles que necessitam de uma "longa viagem" para chegar à empresa, o qual refletiu na qualidade de vida de quem utiliza esse método. Sobrou mais tempo para a família, lazer, prática de esportes e projetos pessoais (AMBITODIGITAL, 2020).

Com o aumento do número trabalhadores em regime de *home office*, aumentou-se também o número de ataques à segurança da informação devido à exploração de vulnerabilidades existentes em um ambiente doméstico.

Um levantamento da Kaspersky, empresa especialista da área de segurança, indica um aumento no registro de domínios suspeitos no primeiro trimestre de 2020 (APOLINÁRIO, 2020). Nesse viés, como as tecnologias atuais podem ser empregadas no contexto de *home office* a fim de melhorar a segurança da informação?

2. Objetivos

2.1. Objetivo Geral

Implementar tecnologias atuais com o objetivo de investigar possíveis melhores configurações que melhoram a segurança da informação em ambientes *home office*.

2.2. Objetivos Específicos

● Configurar VPN em um sistema operacional;

● Criar Políticas de Senhas;

● Configurar Criptografia;

● Configurar Firewall;

● Configurar Antivirus;

● Realizar Backup na Nuvem.

3. Justificativa

Devido a pandemia do novo coronavírus, houve uma alta tanto no índice do trabalho remoto, quanto no índice de ataques de hackers. Este último evento resultou no aumento em perdas e roubos de dados, trazendo prejuízos tanto para as empresas como para os seus funcionários (APOLINÁRIO, 2020).

Por esse motivo, todo investimento em segurança da informação é urgente. O presente estudo visa mostrar como a utilização de tecnologias atuais, que promovem a segurança da informação, podem influenciar no aprimoramento da segurança de um ambiente *home office*.

4. Fundamentação Teórica

4.1. Home Office

O termo *Home Office,* traduzido do inglês, significa “escritório em casa”. Também conhecido como trabalho remoto ou “teletrabalho”, é um meio de um profissional exercer o seu trabalho à distância através da internet desde que não necessite estar presente fisicamente. A SOBRATT - Sociedade Brasileira de Teletrabalho e Teleatividades define teletrabalho como:

> O teletrabalho é a modalidade de trabalho, que utilizando as tecnologias da informação e das comunicações (TIC), pode ser realizada à distância, fora do âmbito onde se encontra o contratante, de maneira total ou parcial, podendo realizar-se em relação de dependência (empregado) ou de maneira autônoma (freelance), executando atividades que podem ser desenvolvidas pelos equipamentos móveis, tais como computadores, smartphones, tablets etc. (SOBRATT, [s.d.]).

No Brasil, o modo de trabalho *Home Office* é relativamente recente e foi reconhecido por Lei em 2011, Lei 12.551 de 15 de dezembro de 2011 (Brasil, 2011). Segundo Castro (2020), após o choque com a pandemia do novo coronavírus, tornou-se bastante procurado que aproximadamente 80% dos executivos que responderam à pesquisa aprovaram esse meio, e mais que 60% acredita que o *Home Office* contribuiu para sua melhoria em eficiência e produtividade, o que antes 51% das empresas não ofereciam essa modalidade de trabalho (CASTRO, 2020).

Contudo, junto ao aumento exponencial do *Home Office,* também cresceu o número de casos de ataques *hackers.*

> [...] os ataques de força bruta (Brute Force Attacks) direcionados ao Remote Desktop Protocol (RDP) – uma das ferramentas de acesso remoto mais populares para postos de trabalho ou servidores – passaram de uma média diária de 402 mil em fevereiro para mais de 1,7 milhão em abril -crescimento de 333% em apenas dois meses (RODRIGUES, 2020).

4.2. Hacker

“Hacker é alguém que aplica habilidades de computação para resolver um problema” (BELCIC, 2020). Muitos quando ouvem a palavra *hacker* já associam, por engano, às pessoas que utilizam do conhecimento de computação para cometer um crime. Todavia, desmentindo o senso comum, existem 3 tipos de *hackers*: o chapéu preto (*black hat*), o chapéu branco (*white hat*) e o chapéu cinza (*gray hat*) (BELCIC, 2020).

4.2.1. Chapéu Preto

Um *hacker* chapéu preto é um cibercriminoso que procura falhas em sistemas e aproveita essas vulnerabilidades para invadir e/ou roubar informações de pessoas e empresas.

> Um chapéu preto é quem viola os sistemas de segurança cibernética para obter acesso ilícito a um computador ou uma rede. Se um hacker chapéu preto descobre uma vulnerabilidade de segurança, ele fará a exploração sozinho ou alertará outros hackers sobre a oportunidade, normalmente em troca de dinheiro (BELCIC, 2020).

Segundo Ivan (2020) "Os hackers *black hat* podem ser tanto amadores iniciantes na disseminação de malware, quanto hackers muito mais habilidosos e experientes que visam roubar informações pessoais, credenciais de login, ou dados bancários".

4.2.2. Chapéu Branco

Um *hacker* chapéu branco é uma pessoa que utiliza de seu conhecimento para tentar invadir um sistema e reportar falhas de segurança à empresa ou pessoa. Muitos desses *hackers* são contratados por empresas para manter os seus sistemas ou redes seguras.

> *Hackers* chapéu branco são o oposto dos *hackers* de chapéu preto. Eles têm os mesmos talentos, mas em vez de usá-los para fins criminosos, eles aplicam esses talentos para ajudar as empresas a fortalecer suas defesas digitais. Um *hacker* chapéu branco tentará intencionalmente violar um sistema, com permissão do proprietário, para identificar pontos fracos a serem corrigidos. Esse tipo de trabalho também é conhecido como "*hacking* ético" (BELCIC, 2020).

4.2.3. Chapéu Cinza

Um *hacker* chapéu cinza é um *hacker* que fica "em cima do muro", ele atua como *white hat* porém em alguns momentos atua como *black hat*, mas sem causar danos muito sérios à empresas ou pessoas.

> [...]Eles não são exatamente o modelo de altruísmo, como os *hackers* chapéu branco, nem se dedicam a atos criminosos. Enquanto os *hackers* chapéus branco obtêm permissão antes de sondar as vulnerabilidades de um sistema, os chapéus cinzas pulam essa parte e vão direto ao *hacking* (BELCIC, 2020).

Para que um hacker consiga realizar um ataque, seja tanto profissional como criminoso, ele busca vulnerabilidades que estão presentes em sistemas ou redes e aplicam técnicas de invasão.

4.3. Vulnerabilidades

Quando um hacker encontra uma vulnerabilidade, ele estuda como utilizá-la para invadir este ambiente. "Uma vulnerabilidade de segurança pode ser vista como qualquer fator que possa contribuir para gerar invasões, roubos de dados ou acessos não autorizados a recursos" (IT.EAM, 2020).

Estando dentro de um sistema já invadido, os hackers estão atentos a buscar novas vulnerabilidades para deixarem uma nova “porta de entrada” facilitada para invasões futuras.

Entretanto, a segurança da informação está aí para evitar esses tipos de cenários com suas propriedades de segurança.

4.4. Segurança da Informação

Segurança da informação ou cibersegurança é a área computacional que foca em guardar e manter os dados de empresas e pessoas seguros sem que terceiros tenham acessos a eles.

> Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas.[...] (KASPERSKY, [s.d.]).

Segundo Mello ([s.d.]), a segurança da informação possui três pilares: Confidencialidade, Integridade e Disponibilidade (MELLO, [s.d.]).

4.4.1. Confidencialidade

A confidencialidade está relacionada à privacidade dos dados, de maneira que ações maliciosas como ataques hackers não liberam informações confidenciais. Uma maneira de reforçá-la é colocando medidas de prevenção, de modo que o acesso só é permitido por pessoas autorizadas (MELLO, [s.d.]).

4.4.2. Integridade

A integridade está associada a confiabilidade dos dados, onde o objetivo é manter os dados da maneira que foram criados. Para as empresas, terem os dados exatos é vantajoso, para que em momento de tomada de decisões os resultados terão uma maior precisão em acertos (MELLO, [s.d.]).

4.4.3. Disponibilidade

A disponibilidade tem o objetivo de manter os dados sempre acessíveis. Uma maneira de segurar que isso aconteça é realizar manutenção rápida de hardware, remover conflitos de software e garantir que os sistemas fiquem atualizados sempre (MELLO, [s.d.]).

A segurança da informação utiliza técnicas e ferramentas para que mantenha as informações seguras, entre elas estão VPN, políticas de senhas, criptografia, Firewall, antivírus, backup utilizando armazenamento na nuvem.

4.5. VPN (Virtual Private Network)

Uma VPN (traduzido do inglês – Rede Privada Virtual) é uma rede privada criada dentro de uma rede pública utilizando os protocolos necessários. Para ter acesso à essa rede, é necessário possuir as credenciais corretas, caso contrário não será possível conectar a ela. “Uma VPN cria um "túnel" pelo qual você pode enviar dados com segurança, usando ferramentas de criptografia e autenticação[...].” (CISCO, [s.d.]).

4.6. Criptografia

A criptografia é um modo de criptografar e descriptografar uma informação, alterando a sua forma original para impossibilitar a leitura por aqueles que não possuem a chave que permite voltar a sua forma original, ou seja, descriptografar a informação. Segundo Ciriaco (2015) “[...]a criptografia é um conjunto de técnicas pensadas para proteger uma informação de modo que apenas emissor e receptor consigam compreendê-la[...]” (CIRIACO, 2015).

4.7. Firewall

Na tradução direta do inglês o firewall significa “parede de fogo”. No conceito de rede de computadores, o firewall sendo um software ou hardware tem o objetivo de filtrar informações que chegam de uma rede, caso o firewall considera o dado como malicioso, ele faz o bloqueio imediatamente garantindo a segurança (COSTA, 2020).

4.8. Antivírus

Os antivírus são softwares desenvolvidos para agir contra vírus durante o início da infecção ou quando se faz uma varredura, podendo eliminar a ameaça ou colocar as mesmas em quarentena onde pode realizar alguma ação posteriormente. Os antivírus são mantidos por empresas da área de segurança da informação (PAULA, 2018).

Segundo Paula (2018):

> Não existe computador imune a vírus, pois a cada dia surgem novos vírus, e leva-se um certo tempo para detectar que o código de um determinado arquivo é destrutivo e seja considerado vírus. Sendo assim, é necessário sempre atualizar o antivírus e evitar a ocorrência de sérios danos ao sistema operacional (PAULA, 2018).

4.9. Backup em Nuvem

Como afirma Goodrich (2019) “O backup na nuvem, também conhecido como backup do computador na nuvem, refere-se ao backup de dados para um servidor remoto baseado na nuvem”. A empresa e/ou usuário que realizar um backup na nuvem pode acessar

os dados remotamente a partir de um login de cliente, geralmente por um navegador web (GOODRICH, 2019).

5. Metodologia

Inicialmente, o tema deste trabalho foi escolhido devido à grande quantidade de empresas que tiveram que partir para a modalidade de trabalho *Home Office* em razão à pandemia do novo coronavírus, além do interesse pessoal pela área de segurança da informação.

Após a escolha do tema, foi realizado o estudo e conceituação de *home office* e segurança da informação e seus princípios básicos através de artigos, sites, documentos e trabalhos relacionados ao tema encontrados na internet.

Estudamos também sobre as principais vulnerabilidades e como os usuários se comportam para favorecerem a fragilidade do ambiente e realizamos uma pesquisa para conhecermos e definir quais tecnologias atuais auxiliam no aumento da segurança da informação em um ambiente *home office*.

Na sequência definimos o sistema operacional que será utilizado no ambiente *home office* e começaremos a prepará-lo, instalando e configurando as tecnologias definidas posteriormente.

Em seguida, começaremos a simular o ambiente *home office* e realizar os testes com as tecnologias e será analisado a eficácia de cada uma.

Na última etapa, será criado um manual de uso das tecnologias implementadas, separadas por uma avaliação de acordo com resultados dos testes realizados. Esta avaliação será classificada em cinco tipos: 5 (Excelente), 4 (Bom), 3 (Médio), 2 (Ruim), 1(Péssimo).

6. Cronograma

ATIVIDADE	Fev	Mar	Abr	Maio	Jun	Jul	Ago	Set	Out	Nov	Dez
Estudo e conceituação de home office e segurança da informação	X	X									
Estudo das principais vulnerabilidades de segurança		X									
Estudo das tecnologias que favorecem a segurança da informação			X								
Definição das tecnologias			X								
Definição do Ambiente				X							
Instalar as tecnologias					X						
Configurar as tecnologias					X	X					
Aplicar testes com as tecnologias simulando um ambiente home office							X				
Análise da eficácia das tecnologias no ambiente home office								X			
Criar o manual de uso das tecnologias									X	X	
Entrega Final											X

7. Resultados alcançados

Na primeira etapa do trabalho, foi realizada uma pesquisa para sabermos como estava a situação do *home office* devido à pandemia do novo coronavírus. Foi realizada também uma pesquisa sobre o aumento de casos de ataques e falhas de segurança relacionados a empresas e trabalhadores que estavam atuando na modalidade *home office*.

Nesta primeira etapa, também foi realizado um estudo das principais vulnerabilidades de segurança que coloca empresas e trabalhadores em risco, tais como a não utilização de uma rede segura, senhas que não possuem uma forte segurança e a inexistência de backups dos dados mais sensíveis.

Com base nas vulnerabilidades de segurança encontradas, foi realizado um estudo sobre quais tecnologias podem suprir essas falhas. Os dados obtidos foram: utilizar VPN para acessar a rede da empresa, utilizar antivírus e mantê-lo sempre atualizado, investir em criptografia de dados, backup de dados e criar uma política de senha para todos os funcionários da empresa.

Em seguida, definimos o sistema que será utilizado como ambiente *home office*. O sistema operacional Windows 10 foi escolhido devido a grande quantidade de usuários que o utiliza, podendo assim englobar uma grande quantidade de pessoas.

8. Resultados esperados

O que se espera deste trabalho é contribuir com o aumento da segurança da informação em ambientes *home office*, o qual irá trazer uma maior credibilidade à modalidade de trabalho, proporcionando uma imagem melhor para as empresas e funcionários que estão inseguros em utilizá-lo.

Referências Bibliográficas

AMBITODIGITAL. **O futuro do Home Office pós-pandemia**. Disponível em: <https://ambitodigital.com.br/o-futuro-do-home-office-pos-pandemia/>. Acesso em: 15 dez. 2020.

APOLINÁRIO, P. **Ataques de hackers aumentaram durante período de home office**. Disponível em: <https://www.revide.com.br/noticias/tecnologia/ataques-de-hackers-aumentaram-durante-periodo-de-homeoffice/>. Acesso em: 10 nov. 2021.

BELCIC, I. **O que é hacking?** Disponível em: <https://www.avast.com/pt-br/c-hacker>. Acesso em: 17 nov. 2020.

BRASIL. **Lei N° 12.551.** MINISTÉRIO DO TRABALHO E EMPREGO - MTE. Brasília, 15 de dezembro de 2011.

CASTRO, N. DE. **É possível conciliar o Home com o Office?** Disponível em: <https://ise.org.br/blog/conciliar-home-office/>. Acesso em: 16 nov. 2020.

CIRIACO, D. **O que é criptografia e por que você deveria usá-la Por Douglas Ciriaco | 19 de Novembro de 2015 às 09h21**. Disponível em: <https://canaltech.com.br/seguranca/o-que-e-criptografia-e-por-que-voce-deveria-usa-la/>. Acesso em: 26 mar. 2021.

CISCO. **Como configurar uma VPN**. Disponível em: <https://www.cisco.com/c/pt_br/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html>. Acesso em: 18 nov. 2020.

COSTA, B. **O que é Firewall**. Disponível em: <https://canaltech.com.br/internet/o-que-e-firewall/>. Acesso em: 29 abr. 2021.

GOODRICH, R. **What Is Cloud Backup?** Disponível em: <https://www.businessnewsdaily.com/5018-what-is-cloud-backup.html>. Acesso em: 3 maio. 2021.

IT.EAM. **Entenda o que é vulnerabilidade de segurança e quais são as mais comuns**. Disponível em: <https://it-eam.com/entenda-o-que-e-vulnerabilidade-de-seguranca-e-quais-sao-as-mais-comuns/>. Acesso em: 15 dez. 2020.

IVAN, G. **Cada hacker com o seu chapéu: o bom, o mau e o feio**. Disponível em: <https://www.avira.com/pt-br/blog/hacker-e-chapeus-black-white-gray-hat>. Acesso em: 10 maio. 2021.

KASPERSKY. **O que é cibersegurança?** Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security>. Acesso em: 19 nov. 2020.

MELLO, A. **Os três pilares da segurança da informação**. Disponível em: <https://ead.catolica.edu.br/blog/pilares-da-seguranca-da-informacao>. Acesso em: 13

maio. 2021.

PAULA, D. P. DE. OFICINA – ANTIVÍRUS. **Instituto Federal Sudeste de Minas Gerais**, 2018.
RODRIGUES, R. **Ataques usando acesso remoto crescem 330% no Brasil**. Disponível em: <https://www.kaspersky.com.br/blog/ataques-rdp-brasil-home-office-pesquisa/15590/>. Acesso em: 15 dez. 2020.

SOBRATT. **Questões**. Disponível em: <http://www.sobratt.org.br/index.php/certificacao/questoes/>. Acesso em: 16 nov. 2020.