CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
CURSO DE GRADUAÇÃO TECNÓLOGO EM REDES DE COMPUTADORES

AYRTON MOURA MOTA
LEONARDO SANTANA MAFRA
NYCOLLAS SALVINO DE OLIVEIRA PONTES

PREVENÇÃO CONTRA ATAQUE DE RANSOMWARE NO PERÍODO HOME OFFICE

RECIFE/2022

AYRTON MOURA MOTA
LEONARDO SANTANA MAFRA
NYCOLLAS SALVINO DE OLIVEIRA PONTES

PREVENÇÃO CONTRA ATAQUE DE RANSOMWARE NO PERÍODO HOME OFFICE

Trabalho Conclusão de Curso apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor(a) Orientador(a): Valfrido Furtado Leite Filho

RECIFE/2022

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 1745.

M917p Mota, Ayrton Moura

Prevenção contra ataque de ransomware no período home office. / Ayrton Moura Mota, Leonardo Santana Mafra, Nycollas Salvino de Oliveira Pontes. - Recife: O Autor, 2022.

26 p.

Orientador(a): Valfrido Furtado Leite Filho.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2022.

Inclui Referências.

1. Home office. 2. Ransomware. 3. Prevenção. I. Mafra, Leonardo Santana. II. Pontes, Nycollas Salvino de Oliveira. III. Centro Universitário Brasileiro - UNIBRA. IV. Título.

CDU: 004

Dedicamos esse trabalho a nossos pais.

AGRADECIMENTOS

Agradeço a Deus por ter nos dado sabedoria, saúde e força para superar todas as adversidades.

Ao nosso orientador, Valfrido Furtado Leite Filho, pelos conselhos e auxílio durante todo o processo.

As nossas famílias e amigos, por nos incentivar, dar carinho e toda a paciência.

A todos que, direta ou indiretamente, fizeram parte da minha formação.

“Ninguém ignora tudo. Ninguém sabe tudo.
Todos nós sabemos alguma coisa. Todos nós

ignoramos alguma coisa. Por isso aprendemos sempre."

(Paulo Freire)

PREVENÇÃO CONTRA ATAQUE DE RANSOMWARE NO PERÍODO HOME OFFICE

Ayrton Moura Mota
Leonardo Santana Mafra
Nycollas Salvino de Oliveira Pontes
Valfrido Furtado Leite Filho

Resumo: A Cada dia percebesse a necessidade de nos aprimorar contra ataques cibernéticos, visto que agora em uma era altamente tecnológica e com capacidade de crescer ainda mais. Nos últimos anos com a chegada de uma pandemia global, na qual existiu a necessidade de isolamento por motivos de saúde. A nova modalidade que cresceu exponencialmente foi o do home office, com isso também cresceram os ataques cibernéticos e um deles em específico foi o Ransomware. O desenvolvimento deste trabalho, tem como objetivo instruir formas de defesa com ataques de Ransomware no ambiente home office. Conclui-se que mecanismos de defesa são essenciais contra ataques de Ransomware no ambiente home office.

Palavras-chave: Home Office; Ransomware; Prevenção.

PREVENÇÃO CONTRA ATAQUE DE RANSOMWARE NO PERÍODO HOME OFFICE

Ayrton Moura Mota
Leonardo Santana Mafra
Nycollas Salvino de Oliveira Pontes
Valfrido Furtado Leite Filho

Abstract: Every day we see the need to improve ourselves against cyber attacks, as we live in a highly technological era with the ability to grow even more. In recent years with the arrival of a global pandemic, in which we found ourselves having to isolate ourselves more at home for health reasons. The new modality that grew exponentially was the home office, with this also growing cyber attacks and one of them in particular was Ransomware. The development of this work aims to instruct ways to defend against Ransomware attacks in the home office environment. It is concluded that defense mechanisms are essential against Ransomware attacks in the home office environment.

Keywords: Home Office; Ransomware; Prevention.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A população mundial tem crescido e com esse crescimento vem surgindo novos problemas que crescem junto e atingem proporções inesperadas, e as pessoas são obrigadas a se adaptar. Em 2020 ocorreu uma pandemia que abrangeu o mundo todo, fazendo com que as pessoas tenham que ficar em casa por motivos de questão sanitária. Uma área que cresceu bastante com isso foi o do Home Office causando o aumento de dados por ataques cibernéticos por *Ransomware.* Em 2020 o Brasil foi o nono país que mais sofreu ataques de *Ransomware* no mundo (mais de 3.800.000 ataques desse tipo) ficando atrás dos EUA, África do Sul, Itália, Reino Unido, Bélgica, México, Holanda e Canadá. (CONVERGÊNCIA DIGITAL, 2022).

Visto isso, se tem a necessidade de melhorar a segurança e privacidade do usuário da rede. O Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021, um aumento de mais de 950% com relação a 2020 (com 8,5 bi), segundo dados apresentados pela empresa *Fortinet*. O Brasil ficou em 2° lugar em toda a América Latina e 5° lugar no mundo, mostrando o quão vulneráveis se pode ficar nessa era tecnológica. "Quase 10% desse ataque global foi direcionado ao Brasil, de acordo com nossos sensores, o que fez do país o principal alvo e trouxe esses números surpreendentes", explica Arturo Torres, estrategista de segurança cibernética do *FortiGuard Labs* da *Fortinet* para América Latina e Caribe. O *FortiGuard Labs* monitora continuamente a superfície de ataque em toda a América Latina e Caribe e, por ter mais de 50% do número de dispositivos de segurança empresarial implantados na região (CONVERGÊNCIA DIGITAL, 2022).

Pode parecer que a proteção de dados e a privacidade na internet são assuntos novos, mas a verdade é que, apesar de terem ganhado bastante popularidade nos últimos anos, eles já são discutidos há décadas. Indica-se que o termo "proteção de dados" começou a ser usado nos anos 60, entretanto a primeira lei foi oficialmente criada ao tema em *Hessen*, na Alemanha, nos anos 70. A Constituição do Brasil, promulgada em 1988, O artigo 5º “são invioláveis a intimidade, a vida privada, a honra

e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". (POLITIZE, 2019)

Em 14 de agosto de 2018 (Lei 13.709), foi sancionada a Lei Geral de Proteção aos Dados (LGPD), no Brasil. Com o objetivo de garantir maior controle dos cidadãos sobre suas informações pessoais, exigindo consentimento explícito para coleta e uso dos dados e obrigando a oferta de opções para o usuário visualizar, corrigir e excluir esses dados (SENADO, 2020).

1.1 Problematização

Este trabalho tem como problema de pesquisa investigar quais os malefícios de um Ransomware dentro do ambiente home office.

1.2 Justificativa

A escolha do tema do trabalho se deu devido a necessidade de informar sobre o risco do Ransomware no período home-office e quais perigos eles oferecem ao trabalhador. A tecnologia é algo que tem crescido exponencialmente e as pessoas devem estar atentas aos benefícios e aos malefícios do mesmo.

Diante disso, este trabalho visa alertar e informar sobre os perigos do Ransomware no ambiente home-office e o que ele pode causar e como ele pode ser evitado para que não cause nenhum mal aos seus dados.

1. 3 Objetivo geral

O trabalho tem como seu principal objetivo apresentar as vulnerabilidades e os métodos de prevenção para garantir a segurança dos dados do seu computador contra ciberataques de *Ransomware* no ambiente *Home Office.*

1.4 Objetivos específicos

- Pesquisar sobre o Ransomware
- Informar sobre o Ransomware no ambiente home office.
- Dados sobre o Ransomware
- Mecanismos de defesa contra o Ransomware.

- Informar como se prevenir contra ataques.

1.5 Metodologia

Nossa metodologia se baseia no fato de que a primeira etapa é a seleção do tema, considerando a escolha do tema ideal. Com isso em mente foi escolhido falar sobre a prevenção de ataques de ransomware no período home office, tendo em vista o número de crescimento de ataques e por experiências relacionadas ao mesmo. Em seguida seguiu para a realização de coleta de dados sobre o tema, por meio de uma documentação indireta com pesquisas bibliográficas de livros como por exemplo: Ransomware: Defending Against Digital Extortion, Ransomware prevention and mitigation techniques, International Journal of Computer Applications. . pesquisas no google acadêmico as quais foram: Funcionalidade de um backup o que é, Segurança no Home office, Mecanismo de defesa contra ransomware Também o uso de sites onde foram encontrados dados que mostravam um exponencial aumento nos casos de 2020 para 2021 de 950%.

2 Sobre o Ransomware

O *Ransomware* é um tipo de software malicioso capaz de infectar, bloquear e sequestrar uma máquina (computador) usando tecnologias de criptografia de dados para impedir que o usuário obtenha acesso ao seu sistema operacional, onde é realizada a prática de extorsão que geralmente é cobrado na maioria das vezes através de criptomoedas “dinheiro digital”, para que o acesso seja restabelecido. (NEVES,2008).

Os ataques de *Ransomware* são bastante utilizados para invadir computadores de grandes empresas, ou de indivíduos com um certo grau de poder aquisitivo com a intenção de captar informações confidenciais. Não há limites para alvo do ataque (LISKA, 2017).

Como pode se espalhar pela internet, o *malware* pode entrar nos sistemas usando “engenharia social, *spam*, *e-mail*, *exploits*, *downloads*, vantagem de vulnerabilidade ou por meio de portas abertas”. Mesmo após a remoção, o impacto do

Ransomware é irreparável e difícil de mitigar sem a ajuda de seus criadores. Esse tipo de ataque tem implicações financeiras imediatas, alimentadas por criptografia de moeda digital. Como resultado, o *Ransomware* se tornou um negócio lucrativo, ganhando popularidade entre os invasores. (NEVES,2008)

Empresas Especializadas em segurança da informação, tais como a *Kaspersky*, *Akamai*, *Sophos*, *Ecoit*, *Norton*, *Malwarebytes*, *Mcafee*, dentre outras, vem se tornando referência na evolução de gerenciamento a vulnerabilidades, tendo em vista a identificação e rastreio de *malwares*. (KASPERSKY, 2019).

2.1 Criptografia

A criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados, aplica-se um algoritmo codificado para que não esteja mais no formato original, portanto, não é legível. Com o uso de uma chave de descriptografia específica os dados podem ser decodificados para o seu formato original. A aplicação de técnicas de codificação faz parte de aspectos importantes da segurança de dados, pois protege informações confidenciais de ameaças, incluindo exploração de *malware* e acesso não autorizado por terceiros. A criptografia de dados é uma solução de segurança geral. Podendo ser aplicada em dados específicos como, senhas ou geralmente todos os dados em arquivos ou contidos na mídia de armazenamento. (LISKA, 2017).

Na necessidade de desenvolver ferramentas capazes de proteger as informações e de preparar a segurança aos dados armazenados e transmitidos pelas organizações através do mundo, enxergou-se a razão de se estudar a criptografia. Dessa forma se pode realizar a criação de novas aplicações que agreguem maior segurança às informações digitais. A criptografia de acordo com o seu conceito e técnicas são utilizadas para codificar e decodificar uma informação, de tal modo que seu real destinatário o emissor da mensagem poderá ter acesso, com a finalidade de evitar que demais pessoas interceptam e entendam a mensagem. Atualmente, existem dois tipos de chaves: a chave pública e a privada. A chave pública é utilizada para codificar as informações, e a chave privada é utilizada para decodificar. Deste modo, na pública, todos têm acesso a determinada aos dados, mas para visualizar os

dados é necessário que o emissor e o receptor autorizem o uso da chave privada. (ALSHAIKH, 2016).

2.2 LGPD

Com o desenvolvimento da globalização e das novas tecnologias, o principal objetivo da Lei Geral de Proteção de Dados (13.709/2018) é proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade das pessoas físicas. Também se concentra na criação de um cenário de segurança jurídica, por meio da padronização de normas e práticas. (SENADO, 2020).

A lei define o que são dados pessoais e explica que alguns deles são de preocupação mais específica, como dados pessoais sensíveis e dados sobre crianças e jovens. Esclareceu também que todos os dados processados em meio físico e digital são regulamentados. Além disso, a LGPD estipula que não importa se a sede de uma organização ou seus data centers estão localizados no Brasil ou no exterior: se for para processar informações sobre pessoas (brasileiras ou não) no país. A lei também autoriza o compartilhamento de dados pessoais com organizações internacionais e outros países, desde que atendidos os requisitos nela estabelecidos. (VALEUPREV,2020).

Antes da lei, as empresas podiam solicitar aos indivíduos (consumidores) ao se cadastrarem para comprar ou prestar serviços uma série de dados que na maioria dos casos, são irrelevantes para o propósito da empresa que os solicita. Muitas vezes, esses dados supostamente confidenciais tornam-se correio comercial. Isso explica por que se passa a receber tantas malas diretas e spams de marcas que não se é consumida e muitas vezes nunca se chega a conhecer. Porém, com a LGPD, isso mudou. Uma vez que a lei entre em vigor, é necessário o consentimento explícito do titular dos dados. Isso significa que os termos de uso e o escopo da autorização devem ser claramente comunicados aos cidadãos, e precisam ser concedidos voluntariamente. As empresas também devem demonstrar que os dados necessários são mais que necessários para se comunicar ou interagir com seus consumidores. (VALUE PREV,2020).

A LGPD se aplica a qualquer operação de tratamento realizado por pessoa física ou jurídica de direito público ou privado, independentemente do meio, do país em que esteja sediada ou do país em que os dados estejam localizados, desde que a operação de processamento de dados ocorra no Brasil. As atividades de tratamento destinam-se ao fornecimento de bens ou serviços ou ao tratamento de dados de pessoas singulares localizadas no país ou ainda o titular dos dados pessoais tratados que tenha sido recolhido em território nacional. (SILVIA BARROS, 2020).

No entanto, com exceção de informações relacionadas à segurança pública, defesa, segurança nacional e repressão investigativa, certos métodos de processamento de dados estão excluídos da aplicação da lei, como o processamento de dados apenas para fins jornalísticos, artísticos e acadêmicos. (DIVERSIDADES, 2018).

3 RANSOMWARE DENTRO DO HOME-OFFICE

O home office (escritório em casa), surgiu na década de 70 e trata-se de uma estrutura de trabalho no ambiente doméstico, mantendo um vínculo empregatício formal com a organização. (RAFALSKI e ANDRADE, 2015) e (BARROS e SILVA, 2010)

Dessa forma, com a abertura de organizações multinacionais de mercados em desenvolvimento e formas de trabalho como o home office, abrem-se oportunidades de internacionalização e descentralização das empresas, criando um cenário com diferentes formas de trabalhar e se apresentarem como uma realidade do fenômeno trabalho. (RAFALSKI e ANDRADE, 2015).

Rodrigues (2020), destaca que com a pandemia COVID-19 afetou empresas de vários segmentos de diversas partes do mundo, têm adotado o home office como modelo de trabalho, porém é necessário realizar este processo de maneira segura do ponto de vista empresarial.

Além do trauma causado pela COVID-19 em 2020. A evolução surpreendente de crimes cibernéticos gerou bastante preocupação na população global. Entre elas o Ransomware, que deixaram de “atirar no escuro” e passaram a ser usadas como arma

contra empresas específicas, principalmente aquelas do setor de saúde e agências governamentais. (CANALTECH,2021)

De acordo com informações levantadas pela ESET **(Empresa Eslovaca de Segurança Cibernética)**, o principal motivo para esse aumento desenfreado no número de incidentes com Ransomware é o despreparo das empresas para lidar com o trabalho remoto. De noite para o dia, escritórios foram fechados e gestores se viram obrigados a mandar suas equipes para trabalhar em casa um ambiente bem mais vulnerável a ataques por conta de uma pandemia global.
(RAMON DE SOUZA, 2021)

Desse modo, a ESET realizou novos questionamentos em dezembro em empresas e órgãos governamentais, situando a preocupação para lidar com a ameaça dos Ransomwares. Segundo estatísticas apresentadas pela ESET, 67% responderam que “apenas algumas empresas”, enquanto 50% acreditavam que “apenas algumas entidades governamentais” têm os recursos para lidar com esse risco.
(CANALTECH, 2021)

Sendo assim, muitas empresas têm sua primeira experiência de trabalho neste cenário que ultimamente vem se tornando desafiador e de paradigma diferente, pois os dados expressos por Rodrigues (2020) também mostram que a falta de aluguel de computadores devido a parte do sistema atual, as empresas não têm experiência em criar políticas de segurança digital para aplicações de forma remota.

Portanto, várias medidas estão sendo tomadas pelas empresas, entre elas a utilização de VPN (Virtual Private Network). Essa é uma das medidas básicas para o funcionamento da empresa diante do novo “normal”. Porque provoca e induz em questões relacionadas à segurança e à disponibilidade segura das informações. (RODRIGUES,2020)

4 MECANISMOS DE DEFESA CONTRA RANSOMWARE

Um ponto importante contra ataques de *Ransomware* são as medidas de defesa, visto que ela tem o objetivo de proteger seu computador e seus dados contra esses ataques.

Uma boa defesa precisa de algumas etapas para aumentar ainda mais a resistência contra esses ataques. (CANALTECH, 2021)

De fato, esses mecanismos são essenciais para impedir que invasores tenham acesso à sua máquina com tanta facilidade. A VPN, atua como um túnel seguro através do qual os dados são transmitidos e copiados com segurança para recuperar e permanecer seguro caso ocorra um ataque ou corrupção de dados. (KASPERSKY, 2021)

4.1 EXEMPLOS DE MECANISMOS DE DEFESA

É importante manter mecanismos de defesas atualizados e em funcionamento para garantir melhor performance na segurança do seu computador e dos seus dados contra possíveis ataques de invasores.

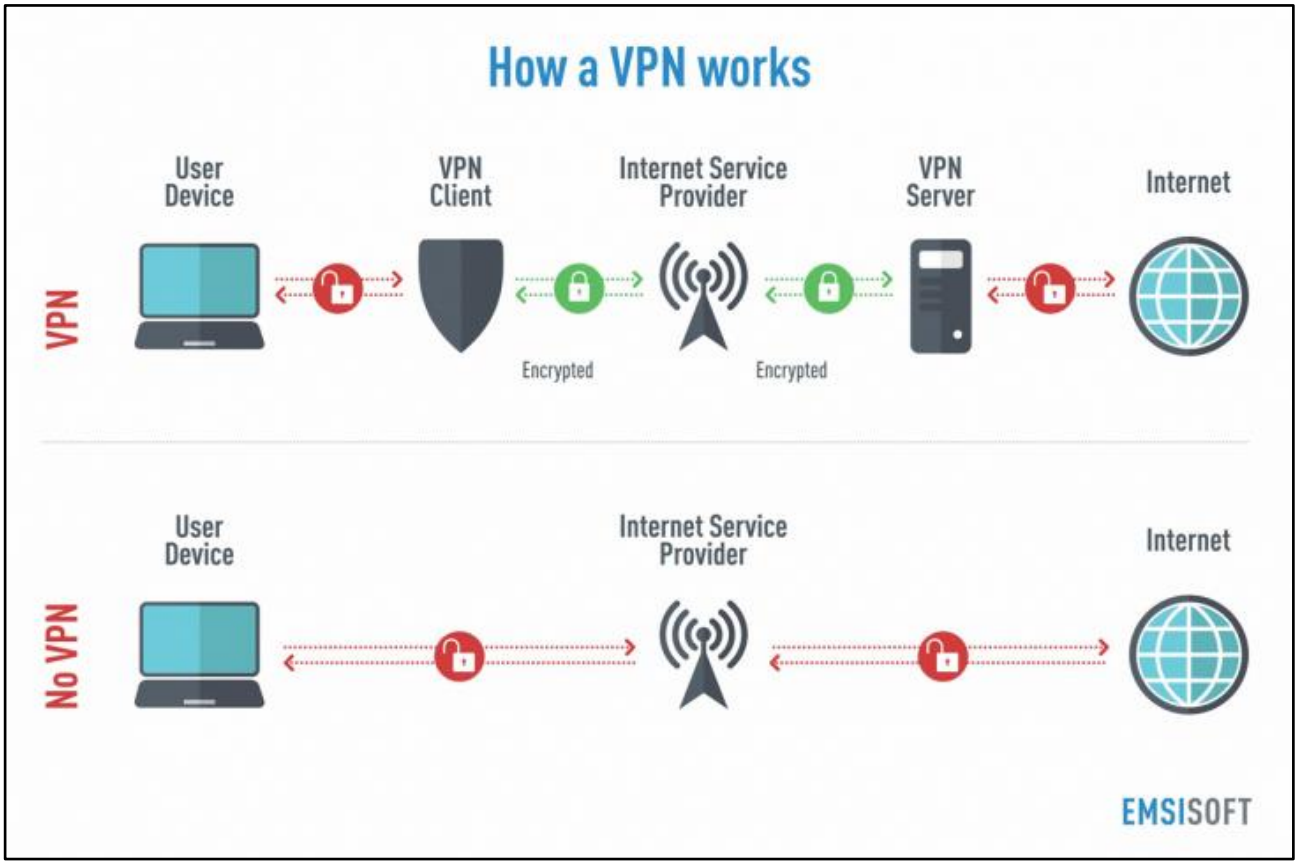
Outro mecanismo de defesa é a atualização dos softwares, firewall e sistema de segurança. Uma das formas de ataque do Ransomware é a exploração da falha do sistema do usuário. Dentro do ambiente Home Office manter os dados do sistema atualizado e os drives é uma boa forma de manter uma defesa, visto que essas atualizações são recomendadas pelo próprio sistema e de fácil operação. (KASPERSKY, 2021)

4.1.1 VPN

VPN (“Virtual Private Network”) (Rede Privada Virtual) é uma ferramenta usada para ter uma conexão segura de rede protegida quando estiver utilizando uma rede pública. A funcionalidade das VPNs é criptografar o tráfego da internet para esconder sua identidade online. Dificultando o acesso a suas atividades e a seus dados. (KASPERSKY, 2017)

Normalmente, quando se vai acessar um site, o provedor de serviços de Internet (ISP) recebe a solicitação e nos redireciona para o destino. Mas quando se conecta à internet com uma VPN, ela redireciona o tráfego da web por meio de um servidor de VPN primeiro, antes de chegar ao seu destino. (KASPERSKY, 2017)

Figura 1. Funcionalidade de uma VPN



(Fonte de imagem: yellowstonecomputing.com)

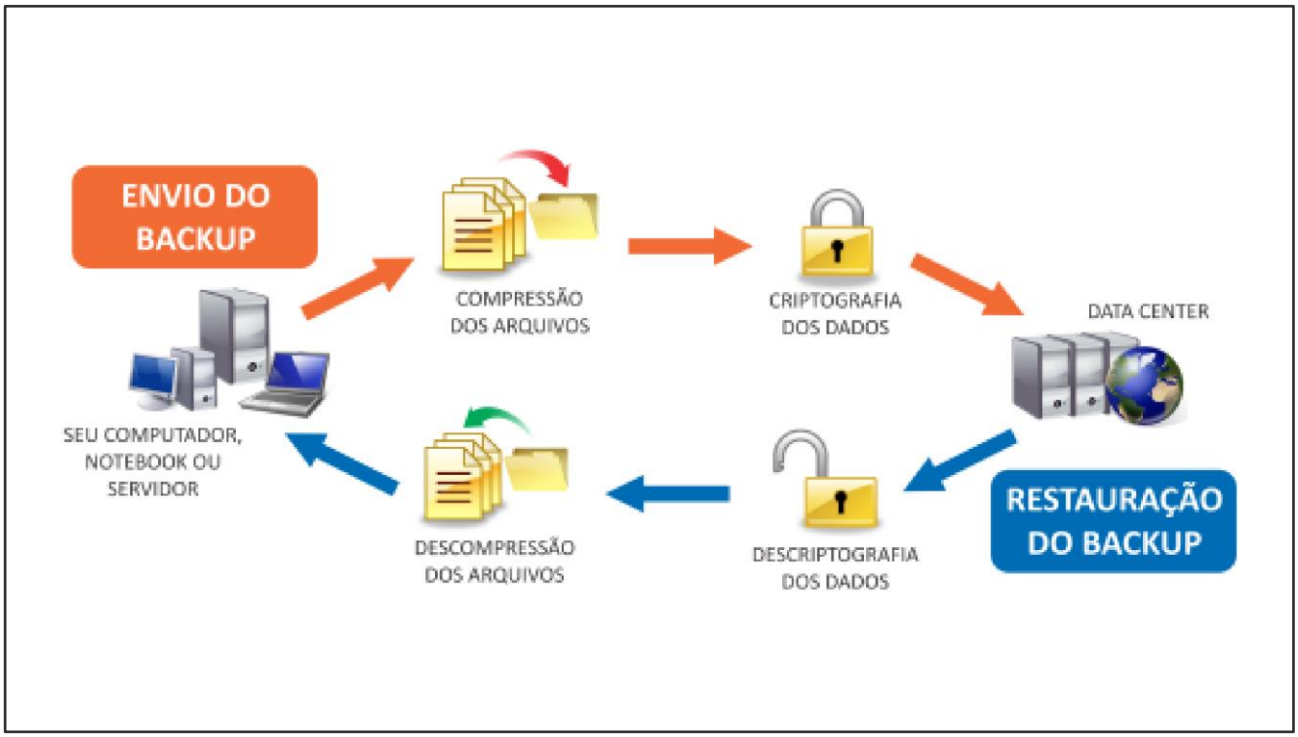
De uma forma simples, a VPN é um túnel pelo qual as informações são transmitidas de forma anônima para que não sejam interceptadas por terceiros. (ROVEDA, 2020)

A rede VPN serve para impedir isso e garantir mais segurança, já que cria um canal de comunicação exclusivo para você, todo criptografado. Ela também camufla o seu IP. Ou seja: é como se você estivesse usando o computador de outro local, com outro IP. (ROVEDA, 2020)

4.1.2 BACKUP

Backup termo usado para “Cópia de segurança” é uma forma de manter seus dados seguros caso perca ou tenham sido roubados. Seja eles (celulares, tablets, computadores) ou sistemas (aplicativos, softwares e jogos).

Figura 2. Funcionalidade do Backup.



(Fonte de imagem: https://gothink.com.br/consultoria-em-ti/backup/)

O computador envia seus dados para um local seguro que poderá ser recuperado caso aconteça alguma coisa com seus dados.(COSSETTI, 2022)

5 LOCAIS PARA ARMAZENAR SEU BACKUP

5.1 PEN DRIVE

Pen Drivers são pequenos dispositivos físicos de entrada USB com capacidade de armazenamento de dados. São bastante versáteis, podendo ser editados e sendo capazes de ser acessados a qualquer hora.

A desvantagem é a capacidade de armazenamento de dados. (MORAES, 2019)

5.2 HD EXTERNO

HDs externos trata-se de dispositivos físicos que são exatamente como dentro de um computador, mas tendo a funcionalidade de ser acessado em qualquer hora e local como um pendrive.

A vantagem é a grande capacidade de armazenamento de dados, sendo melhor que o pendrive. (MORAES, 2019)

5.3 NUVEM

A nuvem se trata de **servidores online** que permitem o armazenamento de dados, sendo não necessário nenhum dispositivo físico.

Alguns dos servidores mais usados são:

- **GOOGLE DRIVE**
- **DROPBOX**
- **ICLOUD**
- **ONE DRIVE**

Esses servidores ficam disponíveis para que se possa recuperar nossos dados a qualquer momento. (MORAES, 2019)

Backups manuais são mais trabalhosos e mais suscetíveis a erros, por isso existem ferramentas de automação para facilitar esse processo.

A maioria dos sistemas operacionais de computador, como o Windows, contam com assistentes nativos que auxiliam você nesse processo.

Alguns dos softwares que ajudam nesse processo são:

- **ACRONIS BACKUP**
- **PARAGON BACKUP**
- **BACKUP MAKER**
- **URANIUM BACKUP**

Uma simples pane em um sistema, por exemplo, pode deletar o registro de toda a sua base de funcionários e clientes. Um ataque de Ransomware pode bloquear o acesso a todas as ordens de compra que tenham sido registradas na sua máquina. (COSTA, 2020)

Por fim, é importante ter uma boa base de backup para recuperar todos dados, sistemas e registros, a fim de superar todas essas adversidades. (COSTA, 2020)

6 AUTENTICAÇÃO DE FATORES

Autenticação de dois fatores 2FA (Two Factor Authentication) é um reforço de segurança contra invasões de contas em redes sociais, como Google e Gmail, para garantir segurança contra a invasão de ataques maliciosos de malwares e hackers. (DIALOGANDO, 2020)

De acordo com o Google, em 2019, a autenticação em dois fatores conseguiu barrar de maneira eficaz até 96% dos ataques e invasões a contas de usuários, porém menos de 10% dos usuários do Gmail (serviço de e-mail do Google) utilizam a função de autenticação em dois fatores. (DIALOGANDO, 2020)

6.1 TIPOS DE FATORES DE AUTENTICAÇÃO

- FATOR DE CONHECIMENTO: Necessário informar algo que o usuário conhece senha ou número de identificação (PIN). (GAVILAN, 2021)
- FATOR DE POSSE: Necessário informar algo que o usuário possui, pode ser carteira de motorista, carteira de identidade, dispositivo móvel ou aplicativo de autenticação. (GAVILAN, 2021)
- FATOR DE CARACTERÍSTICAS: Necessário informar algo que o usuário é geralmente feito de modo biométrico. Pode ser feito por digital, reconhecimento de voz e facial.(GAVILAN, 2021)
- FATOR DE LOCALIZAÇÃO: Acontece geralmente quando o usuário usa em vários locais diferentes o aplicativo em questão. (GAVILAN, 2021)
- FATOR DE TEMPO: Acontece geralmente quando o usuário tenta utilizar fora do horário pré determinado. (GAVILAN, 2021)

Visto isso, entende-se que ativar a autenticação de fatores auxilia a manter as pessoas protegidas e com a proteção próxima delas e de fácil controle contra ataques maliciosos. (AYRES, 2021)

7 RECOMENDAÇÕES DE PREVENÇÃO

Com o aumento dos ataques cibernéticos, a necessidade de defesas se fez ainda mais necessárias. Existem alguns métodos para evitar e auxiliar nessa defesa. (KASPERSKY, 2022)

7.1 EVITAR E-MAILS MALICIOSOS

Atente-se a sempre verificar qual o nome e o email do remetente, normalmente o remetente e o email de resposta são diferentes.(UNIFESSPA,2016)

Quando Receber um Anexo certifique-se de que é algo que você reconhece Arquivos com Finalização de extensão de arquivo .bat, .scr foram alguns dos arquivos conhecidos por conter virus.Se não tiver ideia do tipo de arquivo não abra. (Psafe,2014)

Pode acontecer do dono da conta remetente que está spamando o vírus por e-mail nem faça ideia.Também se faz uso de uma tática de deixar alguns nomes de extensões de arquivos como .pdf .doc mais o arquivo tem seu tipo indicado pelo último ponto normalmente em arquivos maliciosos (.exe).(Psafe,2014)

7.2 PENDRIVE

Uma ótima tecnologia disponível para proteção de dispositivos contra os pendrives são os antivírus com foco em combate a malwares ‘autorun’,que é um tipo de vírus executado quando o dispositivo é conectado via USB. Ele fica varrendo os dispositivos usb e verifica as ameaças. (ALVES,2022)

Uma ótima medida de prevenção é a desativação de execução automática no seu sistema operacional, Um pendrive mesmo conectado ao dispositivo só faz o ataque quando os arquivos infectados são executados. Com essa medida de desligamento dessa função o usuário estará protegido. (SANTOS, 2022)

7.3 ANTIVÍRUS

Uma das ferramentas mais importantes também é o antivírus que é um software com a finalidade de proteção cheio de recursos para deixar o usuário mais seguro. Ele tem o poder de fazer varreduras na sua rede e procurar potenciais arquivos maliciosos ele consegue após identificar eliminar ou mandar o arquivo para aba de quarentena. (HENRIQUES, 2021)

Um dos melhores aliados para sua proteção no home-office com certeza é o antivírus, Fazer uma varredura antes de uma jornada de trabalho é a recomendação mais valiosa com relação ao uso do deste software.(ALMEIDA, 2020)

8 CONSIDERAÇÕES FINAIS

Esta pesquisa falou sobre o Ransomware no período home office, sobre o Ransomware e as formas de defesa contra esse ataque, visto que esse malware tende a crescer e deve-se evitar esse tipo de ataque.

Isto é, o Ransomware é capaz de criptografar arquivos, aplicações e sistemas. Assim que esse Vírus entra no local em questão ele bloqueia causando um dano imensurável a vítima desse ataque.

Como foi observado, no modo de trabalho home office, os funcionários estão conectados a redes diferentes e acabam ficando mais vulneráveis por não possuírem os mesmos equipamentos de proteção que possuem no escritório com dispositivos mais potentes.

Foi necessário entender o funcionamento do Ransomware, suas formas de ataque e como ele funciona depois de aplicado, visto as vulnerabilidades apresentadas no home office.

Tendo em vista que foram mostradas as formas de defesa contra o Ransomware, existem ferramentas e medidas que podem ser tomadas para evitar

cair nesse tipo de ataque malicioso tais como Backup e VPN. Não uso de dispositivos de armazenamento de terceiros ,e-mails maliciosos e uso de antivírus.

Portanto, entende-se que a defesa contra ataques de Ransomware é de extrema importância para manter seus dados em segurança. Como dizia o pensador Wando Elmo “sistema seguro é aquele que não está inseguro! ”.

Após a pesquisa chegamos a conclusão de que a melhor forma de proteção contra o ransomware é manter seus dados protegidos com atualizações e ter um bom Backup.

9 REFERÊNCIAS

ALMEIDA, Abraão. **Segurança Digital: como garantir durante o home office?** 2020. Disponível em: https://blog.hosts.green/seguranca-digital/. Acesso em: 25 jun. 2022.

ALVES, Paulo. **Três dicas para evitar que um pendrive com vírus infecte o PC**. Disponível em: https://www.techtudo.com.br/dicas-e-tutoriais/2018/08/tres-dicas-para-evitar-que-um-pendrive-com-virus-infecte-o-pc.ghtml. Acesso em: 25 jun. 2022.

ALSHAIKH, H.; RAMADAN, N.; HEFNY, H. A. **Ransomware prevention and mitigation techniques. International Journal of Computer Applications**, v. 177, n. 40, p. 31–39, Feb. 2020. Disponível em: . Acesso em: 22 jun. 2022. Citado 3 vezes nas páginas 8, 9 e 10.

DARGAHI, T. et al. A cyber-kill-chain based taxonomy of crypto-ransomware features. Journal of Computer Virology and Hacking Techniques, v. 15, n. 4, p. 277–305, Dec 2019. ISSN 2263-8733. Disponível em: . Citado 2 vezes nas páginas 12 e 13.

ARTIGO QUINTO, **Privacidade: qual sua importância e o que diz a constituição?** 2019. Disponível em: <https://www.politize.com.br/artigo-5/intimidade/#:~:text=%E2 %80%9CS%C3%A3o%20inviol%C3%A1veis%20a%20 intimidade%2C%20a,moral

%20decorrente%20de%20sua%20viola%C3%A7%C3%A3o%E2%80%9D.>

Acessado em: 3 mai. 2022

ASSIS E MENDES, **Proteção de dados: Venda de dados passa a ser legal na Califórnia.** 2019. Disponível em: <https://assisemendes.com.br/tag/privacidade-online/.> Acessado em: 3 mai. 2022

AYRES, Julia. **O que é autenticação de dois fatores (2FA) e por que ela é importante para a segurança dos dados dos seus clientes?** 2021. Disponível em: https://www.infobip.com/pt/blog/o-que-e-autenticacao-de-dois-fatores-2fa. Acesso em: 22 maio 2022.

CANALTECH, **Ransomware segue com a maior ameaça digital no mês de maio.** 2021. Disponível em: < https://canaltech.com.br/seguranca/ransomware-segue-como-a-maior-ameaca-digital-no-mes-de-maio-186988/ .> Acessado em: 8 mai. 2022

CONVERGÊNCIA DIGITAL (Brasil). Convergência Digital. **Ataques malware crescem 61,4% e Brasil sofre 33 milhões de invasões ransomware**. 2022. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Ataques-malware-crescem-61%2C4%25-e-Brasil-sofre-33-milhoes-de-invasoes-ransomware-59488.html?UserActiveTemplate=mobile%2Csite. Acesso em: 25 maio 2022.

CONVERGÊNCIA DIGITAL**, Brasil sofreu 500 bilhões de tentativas de ataques DDoS em 2021,** 2022. Disponível em: <**Erro! A referência de hiperlink não é válida.**.> Acessado em: 10 mar. 2022.

DANIEL,moraes, **O que é backup e como fazer a cópia de segurança das informações.** 2019. Disponível em: <https://rockcontent.com/br/blog/backup/.> Acessado em: 18 abr. 2022

DIALOGANDO,vivo, **Como funciona a autenticação em dois fatores?** 2020. Disponível em: <https://www.dialogando.com.br/seguranca/como-funciona-a-autenticacao-em-dois-fatores.> Acessado em: 1 mai. 2022

DIVERSIDADES (Brasil). Diversidades. **Como a lei de proteção de dados (LGPD) impacta a sua vida**: saiba do que se trata a lei geral de proteção de dados. Saiba do que se trata a Lei Geral de Proteção de Dados. 2021. Diversidade Notícias e Variedades de Macaé. Disponível em: https://www.divercidades.com/colunistas/e-direito/como-lei-de-protecao-de-dados-lgpd-impacta-sua-vida. Acesso em: 21 abr. 2022

GAVILAN, Marcos. **O que é Autenticação de Dois Fatores?** 2021. Disponível em:

https://amt.com.br/o-que-e-autenticacao-de-dois-fatores/. Acesso em: 8 maio 2022.

GOVERNO FEDERAL, **Lei Geral de Proteção de Dados Pessoais, (LGPD)**, 2020. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd.> Acessado em: 6 abr. 2022.

GRUSTNIY, Leonid (ed.). **A saga do ransomware**: ransomware, outrora representados como quase inofensivos, atingiram a maioridade e tem de ser levados

a sério.. Ransomware, outrora representados como quase inofensivos, atingiram a maioridade e têm de ser levados a sério.. 2021. Disponível em: <https://www.kaspersky.com.br/blog/history-of-ransomware/17280/#:~:text=1989:%20O%20primeiro%20ataque%20de,conhecido%20como%20o%20Trojan%20AIDS.> Acesso em: 10 abr. 2022.

HENRIQUES, Pedro. **Você sabe a importância de ter um antivírus?** 2021. Disponível em: https://indicca.com.br/importancia-de-ter-um-antivirus/. Acesso em: 26 jun. 2022.

JUSBRASIL, **A quem se aplica a lei geral de proteção aos dados?,** 2020. Disponível em: < https://silviaslvm.jusbrasil.com.br/artigos/835920387/a-quem-se-aplica-a-lei-geral-de-protecaode-dados-lgpd.> Acessado em:12 abr. 2022

KASPERSKY. **Proteção contra ransomware: como manter seus dados seguros em 2022**. 2021. Disponível em: https://www.kaspersky.com.br/resource-center/threats/how-to-prevent-ransomware. Acesso em: 13 de maio de 2022.

KASPERSKY. **Proteção contra ransomware: como manter seus dados seguros em 2022**. 2021. Kaspersky. Disponível em: Saiba mais sobre a prevenção e a proteção contra ransomware em 2021. Acesso em: 24 maio de 2022.

KASPERSKY DAILY, **O que você precisa saber sobre VPNs.** 2017. Disponível em: <https://www.kaspersky.com.br/blog/vpn-what-you-need-to-know/7225/.> Acessado em: 12 abr. 2022

KHARAZ, A. et al. **UNVEIL: A large-scale, automated approach to detecting ransomware**. In: 25th USENIX Security Symposium (USENIX Security 16). Austin, TX: USENIX Association, 2016. p. 757–772. ISBN 978-1-931971-32-4. Disponível em: . Citado na página 13.

LISKA, A.; GALLO, T. **Ransomware: Defending Against Digital Extortion**. [S.l.]: O'Reilly, 2016. Citado 3 vezes nas páginas 10, 11 e 13.

NEVES, Andressa. **Como evitar se tornar uma vítima de ransomware?**: confira nossas dicas. Confira nossas dicas. 2017. Canaltech. Disponível em: https://canaltech.com.br/seguranca/como-evitar-se-tornar-uma-vitima-de-ransomware-confira-nossas-dicas/. Acesso em: 22 maio 2022.

MISAGHI, Mehran**. Avaliação de Modificações do Cifrador Caótico de Roskin**. Florianópolis, 2001. Dissertação (Mestrado em Ciência da Computação) – Centro Tecnológico, Universidade Federal de Santa Catarina.

MINISTÉRIO DA CIDADANIA (Brasil). Casa Civil da Previdência da República. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Ministério da Cidadania.

Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd. Acesso em: 04 de maio de 2022.

PARÁ. UNIFESSPA. **Dicas para identificar emails fraudulentos**. 2016. Disponível em: https://ctic.unifesspa.edu.br/ultimas-noticias/243-dicas-para-identificar-emails-fraudulentos.html. Acesso em: 25 jun. 2022.

PSAFE. **5 dicas para não abrir e-mail com vírus**. 2014. Disponível em: https://www.psafe.com/blog/seguranca-mail-5-maneiras-certificar-nao-esta-abrindo-virus/. Acesso em: 25 jun. 2022.

SANTOS, Luís. **Alerta de ataque de USB: maneiras fáceis de prevenir ataques de USB**. 2022. Disponível em: https://recoverit.wondershare.com.br/usb-recovery/prevent-usb-attack.html. Acesso em: 23 jun. 2022.

SENADONOTÍCIAS, **Lei Geral de Proteção de Dados entra em vigor Fonte: Agência Senado**, 2020. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor#:~:text=A%20LGPD%20(Lei%2013.709%2C%20de,corrigir%20e%20excluir%20esses%20dados.> Acessado em: 01 abr. 2022

SILVIA BARROS. Jus Brasil. **A quem se aplica a Lei Geral de Proteção de Dados (LGPD)?** 2020. Disponível em: https://silviaslvm.jusbrasil.com.br/artigos/835920387/a-quem-se-aplica-a-lei-geral-de-protecaode-dados-lgpd. Acesso em: 23 abr. 2022.

RAMON DE SOUZA (Brasil). Canaltech (ed.). **Aumento em casos de ransomware está ligado ao home office, afirma ESET**. 2021. Canaltech. Disponível em: https://canaltech.com.br/seguranca/aumento-em-casos-de-ransomware-esta-ligado-ao-home-office-afirma-eset-177682/. Acesso em: 8 jun. 2022.

TANENBAUM, Andrew S. **Redes de Computadores**. 5 ed.. Rio de Janeiro: Campus, 2011.

VALUEPREV, **O que é LGPD e para que serve?** 2020. Disponível em: <https://valueprev.com.br/noticias/o-que-e-lgpd-e-para-que-serve/.> Acessado em: 22 abr. 2022