

SOLUÇÕES DE SEGURANÇA DA INFORMAÇÃO DE BAIXO CUSTO PARA PEQUENAS EMPRESAS PARA PREVENÇÃO DE ATAQUES DE RANSOMWARE

Ranerson José Alves Landim, Daves Marcio Silva Martins

Instituto Federal de Educação, Ciência e Tecnologia do Sudeste de Minas Gerais
(IF Sudeste MG) – Juiz de Fora – MG – Brasil

{ranersonlandim@gmail.com, daves.martins@ifsudestemg.edu.br}

Abstract.

The attack on data hijacking information systems has been growing exponentially, this type of attack is done with ransomware-type malware. The purpose of this attack is to encrypt all files on a company's computer or server, causing the victim to turn to the criminals responsible for the attack to pay to get their data back. There are solutions available to be implemented to prevent this type of tragedy from happening, but small businesses do not have many financial resources to allocate the information security part, so there was a need to implement low-cost information security techniques to prevent ransomware attacks.

Keywords:

Ransomware, Network Computer, Cyber Security, Information Security

Resumo.

O ataque a sistemas de informação do tipo sequestro de dados vem crescendo exponencialmente, esse tipo ataque é feito com *malwares* do tipo *ransomwares*. O objetivo deste ataque é fazer com que seja criptografado todos os arquivos do computador ou servidor de uma empresa, fazendo com que a vítima recorra aos criminosos responsáveis pelo ataque para obter seus dados de volta. Existem soluções disponíveis para serem implementadas para que se evite que aconteça esse tipo de tragédia, porém, pequenas empresas não dispõem de muitos recursos financeiros para destinar a parte de segurança da informação, logo, existe a necessidade de se implementar técnicas de segurança da informação para prevenção contra ataques de *ransomwares*, preferencialmente de baixo custo.

Palavras-Chave:

Ransomware, Redes de Computadores, Segurança da Informação, Cibersegurança

1. Introdução

Diversas empresas pequenas têm enfrentado problemas em manter seus sistemas seguros contra ciberataques, a justificativa pode estar ligada a falta de investimento no setor de segurança da informação (BRANCO, 2021).

Um dos principais tipos de ciberataques que vem preocupando as empresas é o sequestro de dados. Frequentemente são vistas notícias de empresas que pararam suas atividades por conta da criptografia de seus dados, e que, para voltar em suas atividades normais, seria necessário o pagamento de um certo valor para a devolução dos seus dados descriptografados.

O sequestro de dados acontece através dos *ransomwares*, que são *malwares* (software ou código malicioso que tem por finalidade comprometer o sistema), que fazem com que o criminoso tome posse dos dados do computador ou servidor da vítima, fazendo com que somente ele tenha acesso e para a vítima recuperar o acesso a seus dados, o criminoso impõe o pagamento para o resgate dos dados.

No trabalho foram implementadas soluções de baixo custo para prevenção de ataques de *ransomware* como: elaboração e implementação de políticas de segurança, aplicação de *patches* de segurança, atualização de sistema operacional, o uso de ferramentas de antivírus e *firewall*.

2. O problema a ser solucionado

Atualmente, um dos maiores problemas na cibersegurança são os ataques em que existe o sequestro de dados (CUNHA, 2021). Essa modalidade de ataque, faz com que o criminoso tome posse dos dados do computador ou servidor da vítima, fazendo com que somente ele tenha acesso. E para a vítima ter acesso a seus dados novamente, o criminoso impõe o pagamento pelo resgate dos dados.

Diante de uma situação como essa, as empresas e agências que são atingidas devem se esforçar para proteger seus sistemas e tomar uma decisão difícil sobre pagar ou não aos criminosos para remover a interrupção (IYENGAR, 2021).

Segundo a AIG (2021), uma das maiores seguradoras do mundo, houve um aumento de 150% nos pedidos de resgate e extorsão entre 2018 e 2020. Os pedidos de resgate agora respondem por um em cada cinco pedidos de seguro cibernético.

Se por um lado, grandes organizações têm sofrido diversos ataques ultimamente, por outro, existem os pequenos negócios que têm se tornado cada vez mais, alvo dos ataques cibernéticos. Segundo reportagem, “estudos revelaram que 25% das pequenas empresas que sofrem algum tipo de ataque cibernético, declaram falência” (SEGS, 2021).

Segundo o Instituto Ponemon (2020), aproximadamente 63% das pequenas e médias empresas sofreram algum incidente com vazamento de dados no ano de 2019.

As principais causas que ocasionaram esses incidentes foram: a perda ou o roubo de equipamentos, seguida por ataques à rede, vulnerabilidades dos dispositivos móveis e e-mails enviados para remetentes errados. Outra constatação alarmante é que, na maioria

dos casos (52%), os dados comprometidos envolviam informações dos clientes.

A invasão, o sequestro de dados e o vazamento de informações de uma empresa e de clientes, muita das vezes pode ser fatal. A resolução desse problema só pode ser resolvida através da prevenção e para prevenção contra ataques cibernéticos é necessário o investimento em segurança da informação.

2.1. Ransomwares

O *ransomware* é um tipo de *malware* (*software* de código malicioso, que também pode ser chamado de vírus) em que cibercriminosos instalam em computadores ou servidores, sem o conhecimento e consentimento de usuários/administradores. Sua finalidade é o sequestro de dados contidos na “máquina” atacada. O *ransomware* também fornece aos criminosos a capacidade de bloquear o sistema atacado e também fazer a criptografia dos dados contidos nela, tudo isso remotamente.

Geralmente, os criadores de um *ransomware* o projetam para se espalhar por uma rede de computadores e se direcionar a servidores de banco de dados contendo arquivos importantes e de necessidade diária de uma organização ou empresa.

É uma ameaça que está se expandindo gradativamente gerando centenas de milhões de dólares de prejuízos em pagamentos de resgate de dados aos cibercriminosos que os criam e em danos e despesas para as organizações afetadas (GRAÇA; SOUZA, 2020).

Para uma melhor explicação do que é um *ransomware*, deve-se entender que seu conceito não é algo novo e pode ter suas origens encontradas no início da década de 1990, quando Joseph L. Popp (biólogo e pesquisador) escreveu os primeiros códigos maliciosos que viriam a infectar computadores, com o intuito de criptografar as suas informações e obter valores financeiros através do desbloqueio das mesmas (FORNAISER; SPINATO; RIBEIRO, 2020).

Naquela época, assim como funciona hoje, o instalador desse *malware* se alojava no sistema e infectava todo o disco rígido e depois de um certo número de inicializações do sistema, o *malware* tornava-se ativo e fazia a criptografia de arquivos do computador infectado.

Os nomes dos arquivos infectados se renomeavam em uma confusão de caracteres aleatórios, tornando impossível trabalhar normalmente com os arquivos. Por exemplo, para abrir ou executar um arquivo, primeiro era necessário descobrir qual extensão ele deveria ter e alterá-la manualmente (RODRIGUES, 2021).

3. Revisão Sistemática

Para o estudo e realização deste trabalho, foi realizada a revisão sistemática em busca de trabalhos e artigos que abordam assuntos sobre segurança da informação, *ransomwares*, segurança em redes de computadores, *cyber security* e políticas de segurança.

Foi utilizado o Google Acadêmico como base de dados para pesquisa e utilizada as *strings*

de busca: ((*cyber security* OR cibersegurança) AND (*ransomwares* OU *ransomware*) AND (*network computer* OR redes de computadores) AND políticas de segurança.

Com a *string* de busca estabelecida, o resultado de artigos encontrados foram de aproximadamente 1.550. Para o estudo do caso e escolha de artigos para a formulação do trabalho, foram realizadas avaliações dos títulos e dos resumos encontrados na busca inicial.

Quando o título e o resumo dos artigos não eram esclarecedores ou havia falta de nexo entre as informações no que se referia a ataques de *ransomwares*, eram descartados. Ao final da revisão, restaram 46 artigos com um alto grau de compatibilidade com a pesquisa, que posteriormente serviram para a elaboração do trabalho.

Depois da leitura e análise, 16 artigos serviram de base para a pesquisa, levando em consideração os seguintes aspectos: sistemas utilizados, idioma, data de publicação (últimos 6 anos) e metodologias aplicadas em sistemas.

Como alguns exemplos para inspiração para o trabalho, são citados os “*Ransomwares: uma ameaça crescente*” (GRAÇA; SOUZA, 2020). Em que são expostos dados dos últimos anos que contam com uma crescente proliferação de diferentes tipos de *malwares* direcionados a usuários comuns e empresas. A escolha deste trabalho teve motivação no foco em que se tem na segurança da informação abordando os *ransomwares*.

Em “Segurança da informação: Ataques *ransomware* e proteção de dados” (PHILOT, Daniel, 2021). O motivo de escolha do trabalho foi a abordagem sobre as definições e características dos ataques de *ransomware*, e os casos reais citados. Demonstrações sobre casos reais engrandecem o trabalho.

Em “Técnicas de Proteção Contra Ameaças Digitais do Tipo *Ransomware* em Plataforma Windows” (PEREIRA, 2021). A escolha de algumas técnicas e ferramentas como a virtualização de um sistema, serviram como inspiração de estudo e aprimoramento no trabalho.

4. Metodologia

A proposta para a resolução do problema apresentado, resultou na implementação de técnicas que vão compor um pacote de soluções de segurança da informação de baixo custo, para que se aplique em pequenas empresas, para prevenção de ataques de *ransomwares*.

Para a criação e aplicação dessas técnicas, foi criado um ambiente virtualizado, para simular o computador no ambiente empresarial.

Na figura 1, é mostrada a tela do software *Oracle VM VirtualBox* (versão 6.1). Esse foi o software escolhido para a virtualização do ambiente. Na mesma figura estão descritas as configurações utilizadas na máquina virtual, configurações essas que são semelhantes a computadores utilizados em pequenas empresas.





 Geral
Nome: TestesSegurança Sistema Operacional: Windows 10 (64-bit) Grupos: SEG2
 Sistema
Memória Principal: 8160 MB Processadores: 2 Ordem de Boot: Disquete, Óptico, Disco Rígido Aceleração: VT-x/AMD-V, Paginação Aninhada, Paravirtualização Hyper-V
 Tela
 Armazenamento
Controladora: SATA Porta SATA 0: WinClient-A-disk001.vdi (Normal, 50,00 GB) Porta SATA 1: [Disco Óptico] VBoxGuestAdditions.iso (58,27 MB)
 Áudio
Driver do Hospedeiro: Windows DirectSound Controladora: Intel HD Audio
 Rede
Adaptador 1: Intel PRO/1000 MT Desktop (NAT)

figura 1. Configurações do ambiente virtual (RANERSON, 2022)

Foi implementada nesse ambiente, as técnicas que mostram como deixar um sistema mais seguro contra os ataques de *ransomware* e para se fazer valer o experimento, foi utilizado o *ransomware WannaCry* para causar um ataque na máquina criada sem a aplicação dessas técnicas para mostrar o dano causado ao sistema e as consequências geradas (OLIVEIRA, 2018).

4.1 Política de segurança: a barreira essencial contra-ataques de ransomware

A política de segurança pode ser definida como a primeira barreira da segurança de informação contra qualquer tipo de dano ao serviço de uma empresa, seja ele físico ou virtual. A política de segurança faz todo o controle e tráfego das informações em uma empresa.

O documento da política de segurança deve, sempre que precisar, ser atualizado. As responsabilidades pela eficiência das políticas de segurança da informação são compartilhadas por todos os profissionais da tecnologia da informação.

O processo de elaboração e implementação deve ser restrito a times específicos, com vasto conhecimento nas principais normas do mercado. Isso dará muito mais abrangência para as práticas adotadas (ITEAM, 2019).

As políticas de segurança têm por princípios básicos a integridade, confidencialidade, disponibilidade, conforme definição da norma ABNT NBR ISO/IEC 27002:2005 “A informação é um ativo que como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente, necessita ser adequadamente protegida” (ABNT NBR ISO/IEC 27002, 2005).

Ativos são definidos dentro da ABNT NBR ISO/IEC 27002:2013 como: Recursos

de Tecnologia da Informação; informações pertencentes, concedidas ou relacionadas aos clientes; informações relacionadas aos colaboradores; informações pertencentes ou relacionadas aos fornecedores; estratégias e decisões da alta administração; informações contábeis; processos internos (ABNT NBR ISO/IEC 27002, 2013).

O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido (BAUER, 2006).

Criei alguns exemplos de pontos a serem descritos na política de segurança de uma empresa, e os descrevo abaixo:

- Definição da rotina de *backup*, e pessoas que estarão aptas a realizá-la;
- Criação de senhas e privilégios administrativos para determinados colaboradores, bem como a orientação de como utilizar suas senhas e informação sobre punição sobre o mal uso das mesmas;
- Utilização da internet e e-mails (deverá ser informado sobre a proibição de abertura de e-mails de remetentes desconhecidos, bem como a abertura de links duvidosos, nessa parte, se alguma ferramenta de prevenção falhar, o colaborador será a linha de frente contra quaisquer tipos de ataques que venha a ocorrer), proibição do uso de e-mail pessoal;
- Proibição de *downloads*, abertura de links e instalação de *softwares* (essa permissão será concedida somente a pessoas autorizadas);
- Orientação sobre o uso de redes sociais e caso a empresa decidir, realizar bloqueio das mesmas;
- Proibição no uso de dispositivos de armazenamento externos;
- Punições caso sejam descumpridas as medidas de segurança.

A complexidade na elaboração da política de segurança vai depender do tamanho da empresa e as tarefas executadas. Vale lembrar que para cada empresa, o caso é diferente e os responsáveis pela elaboração da política de segurança devem aplicá-la de acordo com a demanda da empresa. Caberá a empresa realizar também uma ação de conscientização com os colaboradores e aliada com o documento da política de segurança, a chance de algum dano proveniente de algum ataque criminoso será mais difícil de acontecer.

4.2. Firewall

Segundo a Cisco Systems (2021), o *firewall* pode ser considerado como a primeira ferramenta na segurança da informação. *Firewall* é um dispositivo de segurança da rede essencial, que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

Ainda segundo a Cisco Systems, os *firewalls* têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas

protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet. Um *firewall* pode ser um *hardware*, *software* ou ambos.

O *firewall*, na forma de *software*, usa um conjunto de regras predefinidas para controlar o tráfego de informações da rede. As regras podem ser alteradas e isso pode ser bom como também pode ser ruim, caso quem for fazer a configuração de *firewall* não tiver domínio sobre o assunto.

É possível interpretar um *firewall* fazendo uma analogia com a forma mais antiga de segurança medieval, que é a criação de um fosso ao redor de um castelo e forçar todos que quiserem entrar a passar por uma ponte levadiça, nessa analogia, o *firewall* seria a ponte levadiça, a única porta de entrada de uma rede (TANENBAUM, 2003).

Aliado ao *firewall*, existem dois recursos que vão complementar ainda mais o seu trabalho de segurança: o IDS (Sistema de Detecção de Intrusão) tem a função principal de identificar e servir como alerta, fornecendo dados sobre as atividades na rede ou em um dispositivo e o IPS (Sistema de Prevenção a Intrusão) que tem a função principal de parar os ataques detectados.

O IDS geralmente não toma uma ação para parar o ataque, ele pode emitir alertas para o administrador, levantar estatísticas e monitorar o tráfego. O resultado dele é uma visibilidade sobre as atividades na rede e nos dispositivos. O IPS, por sua vez, tem função ativa na proteção contra tentativas de ataque. Ele analisa as movimentações na rede e, se detectar um evento suspeito, bloqueia a atividade. (ALLEASY, 2018).

Outra ferramenta importante que também vai se encaixar na parte de *firewall*, é o *webfilter* (filtro de navegação) que faz a proteção interna da rede, já que nem todas as ameaças são externas, muitas vem de dentro da própria rede através dos usuários que podem navegar em sites de forma descoordenada. O filtro de navegação vai executar o monitoramento dos sites e decidir o que pode ou não ser acessado.

4.3. Atualizações de sistema e patches de segurança

Os sistemas operacionais surgiram com dois objetivos principais: criar uma camada de abstração entre o *hardware* e as aplicações, e gerenciar os recursos de maneira eficiente e transparente ao usuário.

Os sistemas operacionais são *softwares* e estão sujeitos às falhas de implementação como qualquer outro, sendo que essas ocorrem dentro do próprio sistema, devido aos erros nas implementações causadas por eventuais deslizos na fase do projeto ou fase de transição do projeto para a codificação (TANENBAUM, FURMANKIEWING, 2006).

É de extrema importância ativar as atualizações automáticas do sistema operacional, pois assim que é liberada uma atualização ou correção de segurança, o próprio sistema se encarregará de realizar e instalar todas as atualizações necessárias.

A atualização dos *softwares* instalados e principalmente do sistema operacional, são fundamentais e trata-se de uma tarefa básica de um administrador da TI. A falta dela é mais recorrente do que possa parecer.

Como foi informado sobre o *ransomware WannaCry* que se espalhou através da falha de segurança do MS17-010 do Windows que explorava a vulnerabilidade no protocolo SMB, enfatiza-se o quão importante e necessário são as atualizações de sistema e dos *patches* de segurança, pois são através dessas atualizações que as falhas são corrigidas e é feita a prevenção contra possíveis invasões (DIORIO, 2019).

O acesso aos serviços por meio de suas falhas ou vulnerabilidades é visto como falta grave e exige atenção especial, pois nestes casos são necessárias as interrupções dos serviços. Os erros em protocolos de comunicação têm que ser monitorados exaustivamente, pois não é possível a interrupção do uso do protocolo de comunicação no sistema, sendo assim, as falhas devem ser isoladas e resolvidas com a máxima prioridade.

Em função de falhas nos protocolos é que são criados os ataques e as invasões mais eficientes, sendo quase imperceptíveis aos dispositivos de segurança que são construídos baseados nestes protocolos. Para estes ataques, o estudo e a análise do comportamento do sistema levam à conclusão que algo está errado, mal intencionado ou é destrutivo (ROCHA et al., 2008).

4.4 Antivírus

Antivírus são sistemas capazes de detectar, bloquear e remover arquivos maliciosos de computadores. Atualmente existem antivírus que são considerados *anti-malwares*, pois além de fazerem a proteção contra vírus são capazes de detectarem outros tipos de arquivos maliciosos como *spyware*, *ransomware*, *phishing* e *trojan*. Os antivírus podem ser baixados nos sites dos seus fabricantes, e, nos sites são descritas as informações das ferramentas, os preços das licenças caso a ferramenta seja paga (ATAIDES, 2018).

Manter um antivírus no dispositivo e mantê-lo atualizado também é uma maneira efetiva para manter o sistema prevenido contra estas ameaças. Geralmente as ferramentas de antivírus já possuem cadastrados em suas bases de dados, os *Ransomwares* já conhecidos e maneiras de detectá-los caso eles invadam o dispositivo (PEREIRA, CASAGRANDE, 2021).

Para o trabalho, houve uma necessidade de escolha de um antivírus que fosse eficiente, e que protegesse contra-ataques de *ransomware*, além de outros tipos de *malwares*. Através das pesquisas realizadas, a ferramenta escolhida foi o antivírus AVIRA.

O *ranking* de antivírus é baseado nos testes realizados pela empresa AV-Comparatives, uma renomada especialista em *softwares* de segurança digital (OFICINADANET, 2022). O AVIRA se sobressaiu em vários testes como: teste de proteção em tempo real, performance, testes de falsos positivos, detecção em arquivos e proteção contra *malware*, justificando novamente a escolha deste antivírus. Nos testes em ambiente controlado, o AVIRA foi utilizado em sua versão gratuita.

4.5 Backup e sua importância contra desastres

Se tratando de tecnologia da informação, imprevistos sempre são esperados, mesmo que

frustrantes do ponto de vista do usuário e preocupantes do ponto de vista organizacional: problemas nos computadores, lentidão nos sistemas e queda nos serviços. Quando tudo parece ter perdido o controle, reiniciar o programa, computador ou dispositivo, pode ser a saída. Independentemente do que pode ter ocasionado a falha, às vezes perde-se dados importantes, obrigando em alguns cenários sua salvaguarda compulsiva, através de backups de arquivos em outros locais ou usar sistemas que fazem essa tarefa de forma automatizada. (SCHNEIER; BRUCE, 2020).

Em novembro de 2020, o STJ foi vítima de um ataque de *ransomware* e teve seus dados e até os *backups* criptografados. De acordo com o CISO Advisor, foram mais de 1.200 servidores infectados que estão com seus dados comprometidos. Os *backups* também foram comprometidos no ataque (THEHACK, 2020).

O *backup*, dentre todos os processos, é o mais importante, seja para prevenir contra ataques cibernéticos, quanto problemas variados como corrompimento de arquivos, falha nos sistemas ou danos materiais.

A recomendação é que esse *backup* seja feito sempre em ambiente externo (na nuvem) ou mídias como *pendrives* e Hds externos, contando sempre com mais de uma opção de *backup*. É de extrema importância também a realização dos testes de integridade (teste de restauração), para analisar se os arquivos podem ser restaurados sem perda de informações.

Vale destacar que o *backup* é extremamente importante e que a rotina de *backup* tem que ser criada para prevenir perdas, pois ao menor sinal de falhas ou ataque no sistema, haverá um ponto a ser restaurado com os dados existentes, porém se tratando de ataques, o *backup* é a última opção a se recorrer, pois se deve evitar de todas as formas disponíveis que o ataque aconteça.

No trabalho, escolheu-se enfatizar técnicas que vão servir para reconhecer e não deixar acontecer o ataque, pois o *backup* só servirá após a falha, e a motivação do trabalho é não deixar que aconteça o ataque de *ransomware*.

A frequência dos *backups* depende da relevância que os dados possuem para a empresa, o que a nível organizacional é 100% relevante ter frequência na realização dos *backups*, seja ele em empresas de pequeno, médio ou grande porte. Essa frequência está ligada a movimentação dos dados, podendo ser diária, semanal, quinzenal ou mensal (FIALHO, 2007).

5. Análises e Resultados

Para análise e demonstração do funcionamento de um *ransomware*, foi o *WannaCry*, que em 2017 foi responsável por um dos maiores ataques de *ransomware* da história, em quatro dias, conseguiu se espalhar por mais de 300.000 sistemas segundo estimativas feitas na época (Oliveira, 2018).

Segundo a Compugraf (2020), empresa no ramo da cibersegurança, mais de 95% de todas as máquinas que foram infectadas, executaram versões sem *patch* de correção do

Windows 7.

O objetivo desse *ransomware* era se instalar em sistemas e servidores e criptografar todos os dados existentes. Logo após do *WannaCry* se instalar no sistema e criptografar os dados, era exibida uma imagem na tela com informações de como realizar o pagamento para poder reaver os dados criptografados.

Na figura 2, está sendo demonstrada a janela que é aberta após o ataque de *ransomware*, nela é solicitado o pagamento através de *bitcoin*, dificultando assim, o rastreamento dos criminosos.

Na figura, o valor cobrado pelo resgate foi de 300 dólares que corresponde a uma fração do *bitcoin*, esse valor pode variar de acordo com o computador e arquivos infectados.



Figura 2: Tela com informações para pagamento do resgate dos dados (GOOGLE IMAGES, 2017)

Segundo a *Microsoft*, o *WannaCry* explorava a falha de segurança do MS17-010 do *Windows* que havia vulnerabilidade no protocolo SMB, no qual sua finalidade é o compartilhamento de arquivos em rede e a permissão para que programas leiam e gravem arquivos e solicitem serviços dos programas do servidor em uma rede de computadores.

A *Microsoft* já havia disponibilizado um *patch* de correção em março de 2017 para a falha MS17-010, o ataque ocorreu em maio do mesmo ano. Dá pra se notar aqui, que houve uma negligência dos administradores de sistema que não atualizaram seus sistemas.

5.1 Análise

No contexto deste trabalho, o *firewall* utilizado foi o do próprio *Windows* (*Windows Defender Firewall*) em conjunto o *firewall* do AVIRA antivírus. Além da proteção contra

ameaças externas, o AVIRA conta com a verificação de *softwares* que precisam ser atualizados. Além do *Windows Update* na realização das atualizações de segurança é feito também o uso do AVIRA para atualizar os demais *softwares* existentes na máquina.

No ambiente de testes criado foi executado o código do *Wannacry* sem as aplicações das soluções descritas neste trabalho. Nenhuma atualização ou *patch* de segurança foi aplicado.

Nesse ponto, ressalto a importância da política de segurança, pois, nesse teste, a falta de implementação da mesma permitiu com que fosse executado o código do *Wannacry*. Com a execução do *ransomware*, o ataque no ambiente criado foi realizado.

O resultado do ataque foi o comprometimento do sistema, a criptografia dos arquivos conhecidos existentes e logo após a execução do *wannacry* houve a troca automática do papel de parede e o surgimento de uma tela com a solicitação de um pagamento de resgate como se vê na figura 3.

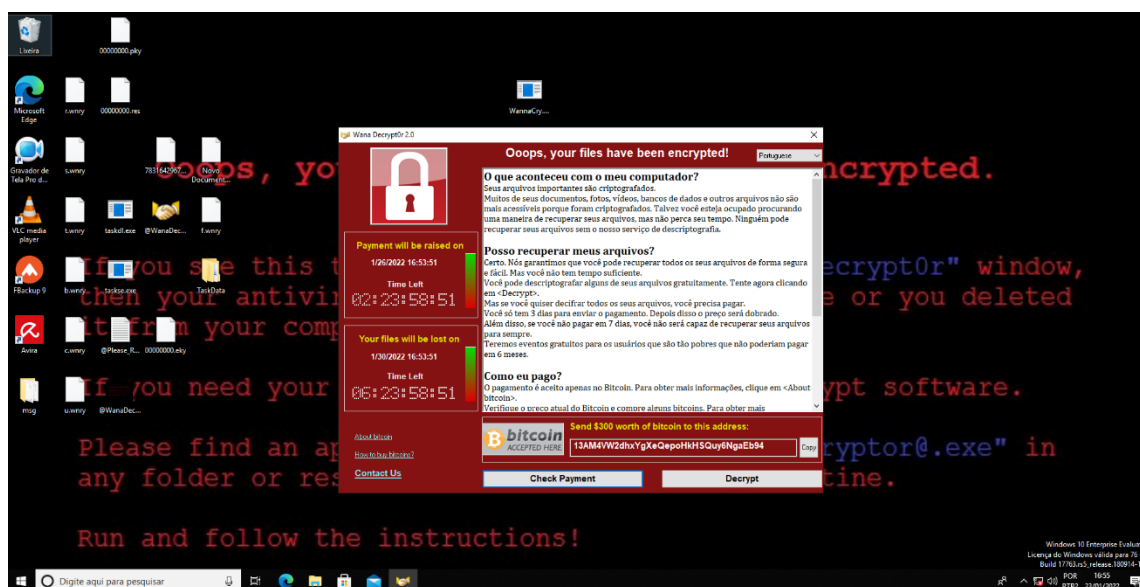


Figura 3: Ambiente de testes comprometido pelo ransomware (RANERSON, 2022)

Quando o sistema sofreu o ataque de *ransomware*, rapidamente foi realizada a criptografia dos arquivos do sistema. Um exemplo disso foram as extensões “.txt” que foram alteradas para “.wannacry”.

A extensão criada após a criptografia pode ser definida de acordo com o que o criminoso desejar, já que essa extensão não fará tanta diferença, ela só serve para mostrar para o usuário que seus arquivos foram criptografados (Oliveira, 2018).

O *WannaCry*, assim como outras variantes de *ransomwares*, após causar a infecção do sistema e criptografia dos arquivos, altera a extensão dos arquivos conhecidos. A figura 4 mostra as extensões de arquivos conhecidos que são alterados após a criptografia do *WannaCry*.

0.123	.bz2	.dotx	.ldf	.odt	.ppt	.sti	.vmdk
.3dm	.cgm	.dwg	.m3u	.onetoc2	.pptm	.stw	.vmx
.3ds	.class	.edb	.m4u	.ost	.pptx	.suo	.vob
.3g2	.cmd	.eml	.max	.otg	.ps1	.svg	.vsd
.3gp	.cpp	.fla	.mdb	.otp	.psd	.swf	.vsdx
0.602	.crt	.flv	.mdf	.ots	.pst	.sxc	.wav
.7z	.cs	.frm	.mid	.ott	.rar	.sxd	.wb2
.ARC	.csr	.gif	.mkv	.p12	.raw	.sxi	.wk1
.PAQ	.csv	.gpg	.mml	.pas	.rb	.sxm	.wks
.accdb	.db	.gz	.mov	.pdf	.rtf	.sxw	.wma
.aes	.dbf	.hwp	.mp3	.pem	.sch	.tar	.wmv
.ai	.dch	.ibd	.mp4	.pfx	.sh	.tbk	.xlc
.asc	.der	.iso	.mpeg	.php	.sldm	.tgz	.xlm
.asf	.dif	.jar	.mpg	.pl	.sldx	.tif	.xls
.asm	.dip	.java	.msg	.png	.slk	.tiff	.xlsb
.asp	.djvu	.jpeg	.myd	.pot	.sin	.txt	.xlsm
.avi	.doc	.jpg	.myi	.potm	.snt	.uop	.xlsx
.backup	.docb	.js	.nef	.potx	.sql	.uot	.xlt
.bak	.docm	.jsp	.odb	.ppam	.sqlite3	.vb	.xltn
.bat	.docx	.key	.odg	.pps	.sqlitedb	.vbs	.xltx
.bmp	.dot	.lay	.odp	.ppsm	.stc	.vcd	.xlw
.brd	.dotm	.lay6	.ods	.ppsx	.std	.vdi	.zip

Figura 4: Tabela de extensões que são criptografadas pelo WannaCry

Em testes, todos os arquivos após serem criptografados e terem suas extensões alteradas, não foram possíveis mais serem abertos, mesmo tentando voltar para sua extensão original.

5.1.2 Resultados e Discursões

A recomendação de especialistas de segurança é que não se pague o resgate, uma vez que fazendo o pagamento, favorecerá o aumento da prática. A primeira coisa a se fazer ao detectar o ataque de *ransomware* é a desconexão do computador da rede para evitar que ele se espalhe e infecte outros computadores (SAISSE, 2016).

Se há o *backup* dos arquivos, pode-se formatar a máquina, reinstalar o sistema operacional e voltar com os dados. Porém se não existe o *backup* ou se há arquivos que ainda não tiverem seu *backup* realizado, pode se partir para o próximo passo que é a tentativa de descriptografia dos arquivos.

Recomenda-se a cópia dos arquivos criptografados, pois as ferramentas de descriptografia podem excluí-los. As ferramentas de descriptografia podem-se encontrar nos sites de antivírus e nos sites *id-ransomware* e *nomore-ransomware*.

Para a recuperação dos arquivos atacados por esse *ransomware*, não houve solução. A recomendação é armazenar o arquivo e esperar por alguma solução futura.

5.2 Resultados

Foi criado um novo ambiente para teste com as mesmas configurações anteriores, agora, aplicando o conjunto de soluções contra o ataque de *ransomware*. Nos testes realizados, foram implementadas as soluções uma a uma, fazendo com que o sistema fosse capaz de neutralizar o ataque.

Como primeira solução, foram feitas todas as atualizações do sistema operacional, antivírus e aplicação dos *patches* de segurança. Com as atualizações, o próprio antivírus e *firewall* do *Windows*, não permitiram a ação do *ransomware* ao ser executado. O AVIRA também informou a ameaça e o mandou para quarentena.

Ressalto a importância da atualização e aplicação dos *patches*, mas ainda assim, não é o bastante. Devido a atualizações e alterações dos códigos de *ransomwares*, novas variantes podem surgir e essas, podem não ser identificadas pelas ferramentas de segurança.

Como outra forma de prevenção, sabendo-se que o *ransomware* reconhece as extensões de arquivos para realizar a criptografia, recomenda-se a alteração das extensões dos arquivos que vão para o *backup*, realizando esse processo, o *ransomware* não conseguirá ter acesso ao arquivo.

A nova extensão a ser renomeada, poderá ser criada pelo administrador do sistema. Por exemplo, fica como recomendação deixar o nome do arquivo e acrescentar um “.@primeironomedousuario123”.

Como solução encontrada, fica como recomendação, a criação de um *script* .bat para a alteração de todos os arquivos da pasta de *backup*. Será necessário a separação dos arquivos por tipo. Após isso, recomenda-se criar um *script* no bloco de notas e salvar como .bat com a seguinte linha de código que terá a função de renomear a extensão existente por uma nova:

```
ren *.txt *.@primeironomedousuario123
```

Feito esse processo, executa-se o arquivo .bat e todas as extensões dos arquivos da pasta serão renomeadas. Nesse teste, os arquivos com a extensão criada não foram criptografados.

Como foi mencionado neste trabalho, nem sempre o antivírus ou *firewall* vão conseguir proteger um sistema 100%. Nesse momento, entram em conjuntos outras técnicas, como por exemplo a política de segurança, pois ela vai ser a primeira barreira contra qualquer tipo de ataque. O fator humano é a principal arma contra ataques externos e internos.

Alguns exemplos de políticas de segurança implementadas, foram o bloqueio de mídias de armazenamento, filtros de sites que podem ser acessados, assim como filtros de *spam*.

A orientação e treinamento de funcionários também entra nesse ponto, e, é um complemento da política de segurança, pois de nada adiantaria realizar todo esse processo, se não há a mínima orientação aos colaboradores da empresa sobre segurança.

Na figura 5 temos um aviso do bloqueio da ação do *ransomware* após a tentativa de execução do mesmo.



Figura 5: Tela de alerta de segurança do antivírus (RANERSON, 2022)

6. Conclusões

O objetivo deste trabalho foi implementar soluções de segurança da informação de baixo custo para aplicação em pequenas empresas, uma vez que muitas dessas empresas não dispõem de muito recurso para investimento em cibersegurança.

Todos os objetivos propostos no trabalho foram alcançados com êxito, desde a revisão da literatura, pesquisa de casos reais de empresas que sofreram com ataques de *ransomware*, até o teste prático, que resultou na eficácia da implementação das soluções descritas, e, que mostrou também, as consequências quando não se tem nenhuma linha de defesa contra ciberataques e principalmente ataques de *ransomware*.

Foi visto como é de extrema importância manter o compromisso com o cuidado para com a segurança da informação, pois não importa o tamanho da empresa, de acordo com o que foi visto, os ataques de *ransomwares* muitas das vezes não são feitos a empresas específicas, e, nesses ataques, quem pode levar mais prejuízo são empresas que não investem em cibersegurança.

Prevenir continua sempre sendo a melhor escolha, é mais seguro e mais barato, pois de acordo com o que foi mostrado, o gasto a se ter depois de um ataque ocorrido, pode ser muita das vezes incalculável.

Referências

ALLEASY. **IDS e IPS: o que é a proteção contra tentativas de ataques?** 27 ago. 2018. Disponível em: <<https://www.alleasy.com.br/2018/08/27/ids-e-ips/>> acesso em: 10 jan. 2022.

ATAIDES, Jeferson de Sousa. **AVALIAÇÃO DE FERRAMENTAS PARA DETECÇÃO DE MALWARES BUSCANDO A SEGURANÇA DE COMPUTADORES EVALUATION OF MALWARE DETECTION TOOLS FOR COMPUTER SAFETY.** 2018.

BAUER, Cesar. **Política de segurança da informação para redes corporativa.** ACADEMIA, mar. 2006.

CANALTECH. **40% das pequenas e médias empresas têm dificuldade de investir em cibersegurança.** Disponível em: <<https://canaltech.com.br/seguranca/40-das-pequenas-e-medias-empresas-tem-dificuldade-de-investir-em-ciberseguranca-199842/>> acesso em: 05 jan. 2022.

CISCO. **O que é um firewall?** Disponível em: <https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html/> acesso em: 11 jan. 2022.

COMPUGRAF. **3 anos do WannaCry: o que aprendemos com um dos worms de ransomware mais agressivos do mundo?** 13 de mai. 2020. Disponível em: <<https://www.compugraf.com.br/3-anos-do-wannacry-o-que-aprendemos-com-um-dos-worms-de-ransomware-mais-agressivos-do-mundo/>> acesso em: 05 dez. 2021.

CUNHA, Lilian. **Por que o Brasil é um dos principais alvos de ataques cibernéticos do mundo.** 11 de dez. 2021. Disponível em: <<https://www.cnnbrasil.com.br/tecnologia/por-que-o-brasil-e-um-dos-principais-alvos-de-ataques-ciberneticos-do-mundo/>> acesso em: 11 jan. 2022.

DIORIO, Rafael Fernando et al. **Ataques em Sistemas e Serviços de Rede Utilizando Exploits Remotos: Um Estudo Prático.** 2019.

FORNAISER, Mateus; SPINATO, Tiago; Ribeiro, Fernanda. **RANSOMWARE E CIBERSEGURANÇA: A INFORMAÇÃO AMEAÇADA POR ATAQUES A DADOS.** REVISTA THESIS JURIS, 03 mar. 2020. e-ISSN: 2317-3580. Disponível em: <<https://periodicos.uninove.br/thesisjuris/article/view/16739/8272ADOS/>> acesso em 10 dez. 2021.

GRAÇA, Douglas Cordeiro da; SOUZA, Rodrigo Vieira. **Ransomwares: uma ameaça crescente.** Trabalho de conclusão de curso (Curso Superior de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana, Americana, 2020.

ITEAM. **Políticas de segurança da informação.** 28 de out. 2019. Disponível em: <<https://it-eam.com/site2021/o-que-sao-politicas-de-seguranca-da-informacao/>> acesso em: 8 jan. 2022.

IYENGAR, Rishi. **Entenda o que é um ataque de ransomware e o que fazer se for atingido.** 05 de jun. 2021. Disponível em: <<https://www.cnnbrasil.com.br/business/entenda-o-que-e-um-ataque-de->

ransomware-e-o-que-fazer-se-for-atingido/> acesso em: 11 jan. 2022.

KINAST, Priscilla. **Ranking: Os 10 melhores antivírus pagos de 2022**. 06 de jan. 2022. Disponível em: <<https://www.oficinadanet.com.br/seguranca/30350-os-melhores-pagos>> acesso em: 07 jan. 2022.

KREBS, Brian. **Spam Nation: The Inside Story of Organized Cybercrime** - From Global Epidemic to Your Front Door. Sourcebooks. 252 páginas.

LISKA, Allan; GALLO, Timothy. **Ransomware: Defending against digital extortion**. Sebastopol: O'Reilly Media, 2016. MARKUS CARPEGIANI DE LEMA e Marcio Freitas, "ATAQUES RANSOMWARE", SGTE, vol. 3, nº 1, maio 2021.

MOZART, Fialho Jr. **Guia essencial do Backup**. Digerati Books, 2007. 128p.

OLIVEIRA, Jéssica Cristina de. **Ransomware: laboratório de ataque do WannaCry**. 2018. 80 f., il. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Software) — Universidade de Brasília, Faculdade UnB Gama (FGA), Brasília, 2018.

PEREIRA, Gabriel F. **Técnicas de Proteção Contra Ameaças Digitais do Tipo Ransomware em Plataformas Windows**. Acesso em: <<http://repositorio.unesc.net/handle/1/8855>> Acesso em: 01 jan. 2022.

PHILOT, Daniel Rocha. **Segurança da informação: ataques ransomware e proteção de dados**. 2021.

RICHARDSON, Ronny – NORTH, Max M. **Ransomware: Evolution, Mitigation and Prevention**. Disponível para download em: <https://digitalcommons.kennesaw.edu/facpubs/4276/> Acesso em: 01 jan. 2022.

ROCHA, Luis Henrique Medeiros da; SOUZA Rodrigo Xavier de; PAREDES, Rogers Vicco; CAMPARI, Wellington; DOBGENSKI, Jeanne. **Uma proposta de gerenciamento de controle de atualizações de segurança de sistemas operacionais**. Revista de Ciências e Tecnologia – Anhanguera Educacional S.A, 2008.

RODRIGUES. R. **Brasil é o 4º país mais atacado por malware financeiro em 2019**. [Brasil] 2019. Kaspersky daily. Disponível em: <<https://www.kaspersky.com.br/blog/brasil-atacado-malware-financeiro-2019-pesquisa/14894/>> Acesso em: 19 dez. 2021.

SCHNEIER, Bruce. **Clique Aqui Para Matar Todo Mundo**: livro didático. 1 ed. Editora Alta Books, 2020.

SAISSE Cabral. **Ransomware: Sequestro de Dados e Extorsão Digital**, RED&TI, vol. 1, nº 6, p. 14, nov. 2016.

TANENBAUM, Andrew S. **Redes de Computadores**. 4ª ed. Rio de Janeiro: Elsevier, 2003.

TECMUNDO. **Brasil é o país mais propenso a sofrer vazamentos de dados em todo o mundo**. Disponível em: <<https://www.tecmundo.com.br/seguranca/154520-brasil-pais-propenso-sofrer-vazamento-o-mundo.htm/>> acesso em: 30 Dez. 2021.

VALUEHOST. **Ransomware: entenda o que é e como se prevenir.** [Brasil] 18 nov. 2019. Disponível em:<<https://www.valuehost.com.br/blog/ransomwarecomo-se-prevenir/>> acesso em: 08 dez. 2021.

YOUNG, Adam, and Moti Yung. "**Cryptovirology: Extortion-based security threats and countermeasures.**" In Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on, pp. 129-140. IEEE, 1996.