PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

VULNERABILIDADE EM REDES DE COMPUTADORES CORPORATIVAS: ESTUDOS DE CASO SOBRE ATAQUES DE RANSOMWARE

MARCO AURÉLIO SIRQUEIRA DE SÁ

GOIÂNIA
2023

MARCO AURÉLIO SIRQUEIRA DE SÁ

VULNERABILIDADE EM REDES DE COMPUTADORES CORPORATIVAS: ESTUDOS DE CASO SOBRE ATAQUES DE RANSOMWARE

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.

Orientadora:

Profa. Dra. Solange Da Silva

Banca examinadora:

Prof. Dr. José Luiz de Freitas Júnior

Prof. Me. Rafael Leal Martins

GOIÂNIA

2023

MARCO AURÉLIO SIRQUEIRA DE SÁ

VULNERABILIDADE EM REDES DE COMPUTADORES CORPORATIVAS: ESTUDOS DE CASO SOBRE ATAQUES DE RANSOMWARE

Este Trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Engenharia de Computação, e aprovado em sua forma final pela Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, em ____/____/_____.

_____

Orientadora: Profa. Dra. Solange da Silva

_____

Prof. Dr. José Luiz de Freitas Júnior

_____

Prof. Me. Rafael Leal Martins

GOIÂNIA

2023

Dedico este trabalho aos meus pais como sinal de gratidão por todo amor e apoio em todas as fases da minha vida.

AGRADECIMENTOS

A Deus por me dar força e saúde para vencer os desafios e por me permitir superar os obstáculos que encontrei durante esta caminhada de estudos.

Gostaria de agradecer minha família, especialmente meu pai Braunilio, minha mãe Lucelma, meus irmãos Marcelo e Nayara, por sempre me apoiarem em todos os momentos de minha vida.

A minha orientadora Solange da Silva, por todo apoio, paciência e por sempre ter me ajudado a realizar cada passo deste trabalho.

A todos que de uma forma ou de outra contribuíram para que este trabalho se realizasse.

RESUMO

O objetivo geral deste trabalho é identificar os principais riscos de segurança em redes corporativas e apresentar como se proteger contra os ataques de *Ransomware.* Quanto aos procedimentos metodológicos esta pesquisa é bibliográfica. Quanto aos resultados foram identificados diversos tipos de ataques de *Ransomware*, e os principais são: *Scareware, Petya, Doxware, Cerber, Ryuk,* SQL *Injection, Phishing e Sniffing.* Os principais pontos de vulnerabilidade identificados foram: falta de conscientização e treinamento adequado dos funcionários, protocolos de segurança fracos e falta de boas práticas no desenvolvimento das aplicações. O estudo permitiu concluir que não existe uma única solução para evitar os ataques e resolver todos os problemas de vulnerabilidades da empresa. Além disso, saber quais são os principais tipos de ataques e como os cibercriminosos agem são fatores importantes para manter a empresa protegida contra ataques cibernéticos. Assim, no contexto atual, é muito importante que as empresas implementem mecanismos de segurança e sigam normas para se protegerem contra esses ataques. As ameaças nesse campo estão se tornando mais complexas, sofisticadas e organizadas, aumentando a importância dessas medidas de proteção. Embora, não exista uma solução única para prevenir todos os ataques e eliminar as vulnerabilidades de uma empresa, existem métodos eficazes de proteção e diretrizes recomendadas, como treinar os funcionários e implementar políticas de segurança consistentes em toda a organização.

Palavras Chaves: Redes corporativas. *Ransomware.* Segurança da Informação. Vulnerabilidades. Ataques Cibernéticos.

ABSTRACT

The main objective of this work was to deepen the understanding of the challenges faced by corporate networks in terms of cybersecurity, with a special focus on the threat of ransomware attacks. To carry out this work, the bibliographic research method was used, using relevant and reliable sources. As for the results, several types of Ransomware attacks were identified, and the main ones are: Scareware, Petya, Doxware, Cerber, Ryuk, SQL Injection, Phishing and Sniffing. And the main points of vulnerability are: lack of awareness and adequate training of employees, weak security protocols and lack of good practices in application development. The results allowed us to conclude that there is no single solution to prevent attacks and solve all the company's vulnerability problems. However, there are several efficient forms of protection and good practices, such as employee training and maintaining widespread security policies within the organization. Furthermore, knowing what the main types of attacks are and how cybercriminals act are factors in keeping the company protected against cyberattacks.

Keywords: Corporate networks. Ransomware. Data security. Vulnerabilities. Attacks. Cybercrime.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

BD	Banco de Dados
DNS	*Domain Name System*
DKIM	*Domain Keys Identified Mail*
FTP	*File Transfer Protocol*
GDPR	*General Data Protection Regularion* ou Regulamento Geral de Proteção de Dados
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
IP	*Internet Protocol* ou Protocolo da Internet
LGPD	Lei Geral de Proteção de Dados Pessoais
NNTP	*Network News Transfer Protocol*
RAM	R*andom Access Memory* ou Memória de Acesso Randômico
SGBD	Sistema Gerenciador de Banco de Dados
SPF	*Sender Policy Framework*
SI	Segurança da Informação
SMTP	*Simple Mail Transfer Protocol*
SO	Sistema Operacional
SQL	*Structured Query Language* ou Linguagem de Consulta Estruturada
SQLi	SQL *Injection* ou Injeção SQL
TCC	Trabalho de Conclusão de Curso
TCP	*Transmission Control Protocol* ou Protocolo de Controle de Transmissão
TI	Tecnologia da Informação
VPN	Rede Privada Virtual

SUMÁRIO

1 INTRODUÇÃO

Com o tempo, as informações se transformaram em um recurso valioso para empresas, agências governamentais e indivíduos. O acesso não autorizado a informações privadas de uma empresa por terceiros pode fazer com que a empresa falhe financeiramente, bem como em sua capacidade de competir no mercado (Brito, 2016).

A Tecnologia da Informação (TI), é o conjunto de todas as atividades e soluções possibilitadas pelos recursos computacionais com o objetivo de possibilitar a aquisição, armazenamento, proteção, processamento, acesso, gerenciamento e uso da informação. Este conjunto de soluções é constituído por uma combinação de equipamentos (*hardware*) e *software* (Alecrim, 2019).

Batista (2004, p. 59), define: “TI é todo e qualquer dispositivo que tenha a capacidade para tratar dados e/ou informações, tanto de forma sistêmica como esporádica, independentemente da maneira como é aplicada”.

A segurança da informação (SI) refere-se à proteção já existente para os dados de uma determinada empresa ou pessoa, ou seja, aplica-se tanto aos dados corporativos quanto aos pessoais. Abrange todas as informações e qualquer conteúdo ou dados que tenham valor para qualquer organização ou indivíduo. Podendo ser guardada para uso restrito ou exibidos para inspeção ou compra pública (Araújo, 2022).

Preocupações com a segurança de informações corporativas, dados pessoais e dados governamentais levaram empresas e o governo a desenvolverem novas medidas de segurança e tributação para o tratamento de dados no Brasil. A Lei nº 13.709, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD), foi instituída em 14 de agosto de 2018 e inclui medidas para proteger a confidencialidade e manutenção de informações de terceiros (Serpro, 2018).

A LGPD, lei criada no Brasil para tratar da proteção de dados pessoais, ela estabelece uma série de requisitos para empresas e organizações em relação à coleta, armazenamento, manuseio e compartilhamento de dados pessoais online e offline (Nones, 2022).

O local onde as informações são armazenadas, compartilhadas e comunicadas online em um domínio de redes de computadores é conhecido como "Ciberespaço". Não apenas virtual, o ciberespaço também incluiu dispositivos físicos

como computadores que armazenam dados e telefones celulares, entre outros (Galoyan, 2019).

Os dados podem ser considerados uma coleção de recursos brutos, que até agora não tem significado. Onde é possível extrair informações específicas desses elementos. Filmes, imagens e livros, entre outras coisas, podem ser considerados como dados (Moreira et al., 2020).

Os dados são vistos como um patrimônio devido ao seu valor estratégico. A segurança dos dados é essencial para as organizações, pois é essencial comunicar a confiança e a integridade dessas informações aos clientes e à área local para empresas que usam processos digitais (Totus, 2020).

Uma rede corporativa de computadores é um conjunto de computadores conectados por uma infraestrutura de comunicação que permite que recursos e informações sejam compartilhados entre dispositivos de rede (Oliveira, 2015).

As redes de computadores desempenham um papel significativo na vida das pessoas, seja no âmbito pessoal ou profissional. Ela é utilizada para possibilitar que as pessoas troquem mensagens, enviem e recebam arquivos como fotos, vídeos, arquivos de áudio e documentos, acessem conteúdo, entre outras coisas (Menezes, 2023).

O termo "*hacker*" refere-se a uma pessoa que estuda linguagens de programação, procura falhas em sistemas que não deveriam ter e tenta obter acesso a dados. Alguns *hackers* usam essas técnicas para o bem, informando as empresas sobre erros e, às vezes, recebendo o pagamento como resultado. Outros, no entanto, aproveitam vantagens sobre essas lacunas para obter acesso aos dados para seu próprio ganho pessoal (Andrade et al., 2017).

Ransomware é um tipo *software* malicioso que infecta computadores e restringe o acesso ao sistema por meio de criptografia. Para restaurar o acesso, o resgate é cobrado pelos criminosos, e normalmente é pago na forma de “moeda digital” (Lara, 2022).

O *ransomware* é uma ciber ameaça comparável a um ataque sem meios tecnológicos, como um sequestro. Ele é um tipo de *software* malicioso, que criminosos instalam em computadores sem o consentimento do usuário, possibilitando o bloqueio remoto do computador. O *ransomware* é um aplicativo que criptografa as informações do computador e inclui uma série de instruções para que o usuário consiga recuperar seus arquivos. De acordo com as instruções do atacante,

a vítima do ataque deve pagar-lhe uma quantia em dinheiro para obter a chave que libera as informações. Essa ameaça geralmente surge quando uma pessoa clica em um link malicioso, abre um anexo de *e-mail* ou abre um anexo mal-intencionado (Neves, 2018).

Ransomwares são usados para invadir computadores pertencentes a grandes corporações ou indivíduos, com poder aquisitivo, a fim de capturar informações confidenciais (Liska, 2017).

O investimento em segurança cibernética tornou-se uma necessidade e um fator de sucesso para as empresas. Além de tornar as organizações mais vulneráveis e colocar seus dados em risco, esses ataques tendem a crescer e a se desenvolverem rapidamente conforme os avanços tecnológicos (Fernandes, 2019).

Justifica-se estudar este tema porque o *ransomware* é um tipo de cibercrime mais rápido e crescente, que acompanha o desenvolvimento tecnológico e está na categoria de cibercrimes que mais crescem. Com isso, as empresas passaram a investir mais em SI, que teve um salto de US $ 325 milhões em 2015 para US $ 20 bilhões até 2020, (Malagutti, 2016). Além disso, operações de negócios e atividades profissionais agora estão sendo realizadas em ambientes online. Com isso, a segurança dos dados aumentou porque essas circunstâncias facilitam o risco à integridade das informações que trafegam na rede (Santiago, 2018). As empresas estão investindo mais em SI, que passou de US 325 milhões em 2015, para US $ 20 bilhões em 2020, isso em todo o mundo. (Malagutti, 2016). Esses tipos de ataques cresceram 311% no ano de 2020, rendendo em torno de US$ 350 milhões a hackers (Arbulu, 2021).

Diante deste contexto, esse projeto visa responder a seguinte questão de pesquisa: **- Quais são os principais riscos de segurança em redes corporativas e como se proteger contra os ataques de *ransomware* em redes corporativas?**

O objetivo geral deste trabalho é identificar os principais riscos de segurança em redes corporativas e apresentar como se proteger contra os ataques de *Ransomware.*

Os objetivos específicos são:

- Analisar as vulnerabilidades mais comuns em redes corporativas;
- Apresentar soluções para mitigar esses riscos.

Espera-se que os resultados deste trabalho possam contribuir:

- Identificação e solução de vulnerabilidades na rede, minimizando o impacto de incidentes de segurança em relação aos *ransomware*;
- Redução significativa dos incidentes de segurança na rede corporativa;
- Informação, ajudando na eficácia dos controles de segurança implementados na rede corporativa;

Esta monografia está estruturada da seguinte forma: neste capítulo é apresentado o contexto do trabalho, a questão de pesquisa, objetivo e resultados esperados. No capítulo 2 é apresentado o referencial teórico com conceitos, definições, leis e normas de proteção aos dados e trabalhos relacionados ao tema. No capítulo 3 é apresentado o método, mostrando como o trabalho foi desenvolvido e o que foi feito para atingir o objetivo geral. No capítulo 4 é apresentado os principais tipos de ataques de *ransomware* aos dados de empresas já conhecidos, identificando as vulnerabilidades que permitiram que o acesso indesejado ocorresse.

2 REFERENCIAL TEÓRICO

Este capítulo está dividido em três partes, a primeira apresenta conceitos e definições necessárias para a compreensão do trabalho, a segunda apresenta algumas leis e normas relacionadas à segurança de dados e a terceira mostra trabalhos relacionados ao tema.

2.1 Conceitos e Definições

Segurança da Informação (SI) nada mais é do que as políticas, procedimentos e métodos que devem ser utilizados para garantir que a circulação de dados e informações sejam seguras e controladas, impedindo o uso ou pelo menos concedendo acesso a indivíduos que não deveriam ter acesso a tais informações (Veloso, 2023).

A SI busca a proteção da informação contra muitos tipos de ameaças aos dados que estão disponíveis para uma organização. Sendo muito debatido em decorrência do avanço da tecnologia, tornando-se cada vez mais significativo para as organizações (Ramos, et al. 2017).

A informação é uma coleção de dados que foram adequadamente organizados e protegidos. Qualquer tipo de informação disponível é produzido, enviado, armazenado, usado, acessado e protegido usando a informação. É por esse motivo

que as políticas de segurança da informação estão surgindo, tendo a prevenção de ataques cibernéticos como um de seus focos principais (Zeferino, 2020).

As medidas abrangentes de proteção de dados da SI são construídas sobre os seguintes pilares: confidencialidade, integridade, disponibilidade e autenticidade. Esses fundamentos são essenciais para a proteção das informações da organização (Durbano, 2018).

Cibersegurança é um conjunto de medidas preventivas destinadas a proteção de pessoas, dispositivos e sistemas contra qualquer tipo de ataque que pode se aproveitar de falhas do sistema, para acessar, roubar e manipular dados. Implica na prevenção e proteção enquanto atua apenas online (Schultz, 2020).

A prática ilegal de usar um computador ou outras ferramentas de TI para realizar atos criminosos em que o equipamento de TI é alvo do crime é conhecido como cibercrime. Onde os criminosos se aproveitam das vulnerabilidades nas redes de computadores para roubar dados, o que pode causar danos significativos às empresas (Fernandes, 2020).

Segundo estudo da *Symantec*, empresa especializada em criar soluções em antivírus em todo o mundo, os brasileiros tiveram um prejuízo de mais ou menos R$ 33 milhões com crimes cibernéticos em 2016. Ou seja, esses crimes afetaram quase 42,4 milhões cidadãos do país (Lucena, 2017).

Operações de negócios e atividades profissionais agora estão sendo realizadas em ambientes online. Com isso, a segurança dos dados aumentou, pois essas circunstâncias aumentam o risco à integridade das informações que trafegam nas redes de computadores (Santiago, 2018).

Na maioria das vezes, as empresas possuem uma variedade de dados e informações que precisam ser organizadas e disponibilizadas para futuras consultas. Dessa forma, um Banco de Dados (BD) armazena, organiza e agrupa esses dados para futura verificação organizacional ou fins de segurança em um domínio específico (Souza, 2020).

A manipulação de um BD é realizada através do Sistema Gerenciador de Banco de Dados (SGBD). Com o SGBD, é possível manipular os dados por meio de uma linguagem como a *Structured Query Language* (SQL) para verificar a integridade, regular permissões e transações, entre outras coisas. Uma delas é o MySQL (Oliveira, 2020).

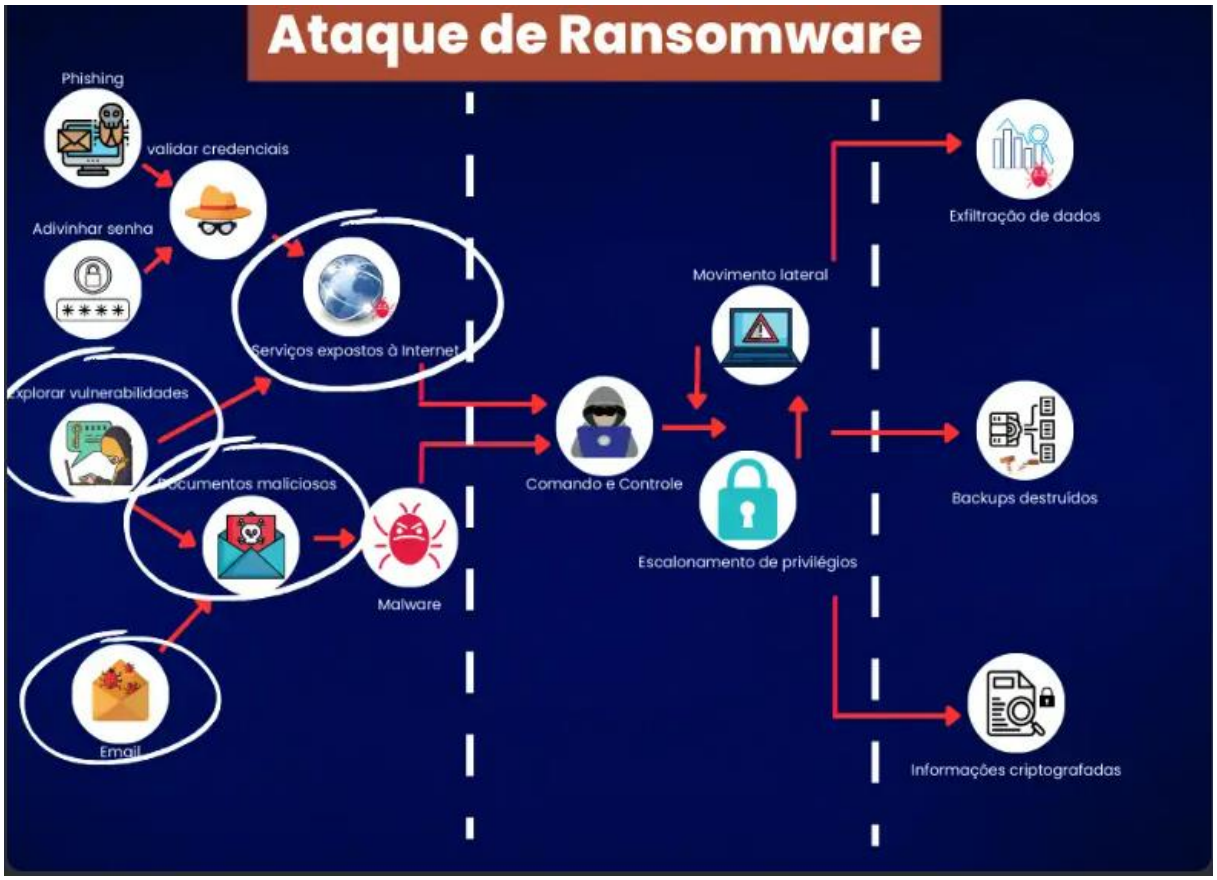
A definição mais simples e que descreve com precisão o que é *ransomware*, é que se trata de um tipo específico de *malware* que nega o acesso de um usuário aos seus dados, criptografando conjuntos de dados inteiros e exigindo um resgate (*ransom*, em inglês) para que o usuário recupere o acesso às suas informações previamente estabelecidas. Essa prática também é conhecida como sequestro digital, mudando o alvo de pessoas para seus dados, que muitas vezes contêm informações vitais para o funcionamento de negócios e outras estruturas organizacionais ou mesmo valor sentimental para a pessoa que o possui (Hassan, 2019).

O primeiro *ransomware* foi criado em 1989 por Jhopeh L. Popp, um biólogo formado em *Harvard*. O vírus foi chamado de “AIDS” e enganava os usuários afirmando que a licença do software havia prescrito. Assim, criptografava os dados no disco rígido e exigia que as vítimas pagassem US$ 189 para desbloquear seus arquivos (Liska, 2017).

A capacidade do *ransomware* de se adaptar a muitos fatores, como tecnologia, segurança, economia e até mesmo a cultura local da vítima, o que diferencia de outras ameaças. Particularmente, no caso da AIDS Trojan, não houve tantos sucessos quanto agora, pois, em 1995, uma grande parte dos usuários eram especialistas em ciência e tecnologia. E o processamento de dados era muito mais difícil e a criptografia não era assimétrica como era em 2018. Em vez disso, a criptografia simétrica foi adotada (Liska, 2017).

O procedimento de ataque do *ransonware* começa quando um sistema é infectado por meio de uma variedade técnicas. Podendo acontecer através de anexos de e-mails maliciosos, *downloads* em sites comprometidos, exploração de vulnerabilidades ou até mesmo enexos em redes sociais (Santos, 2023), conforme mostra a Figura 1.

Figura 1 – Procedimento de ataque do *Ransomware*.



Fonte: Dio.me (2023).

Segundo Tavella (2021) as principais características do *ransomware* são:

1. Criptografia de arquivos: O *Ransomware* criptografa os arquivos do sistema ou do usuário, tornando-os inacessíveis sem a chave de descriptografia. Os cibercriminosos mantêm essa chave e a oferecem em troca de pagamento.
2. Resgate em Moeda Digital: Normalmente, os criminosos solicitam o pagamento do resgate em criptomoedas, especialmente Bitcoin. Isso dificulta o rastreamento das transações e fornece anonimato aos criminosos.
3. Ameaças e alertas: Após criptografar os arquivos, o *Ransomware* exibe mensagens de resgate na tela da vítima, geralmente com prazos para pagamento e ameaças de que os arquivos serão perdidos permanentemente se o resgate não for pago.

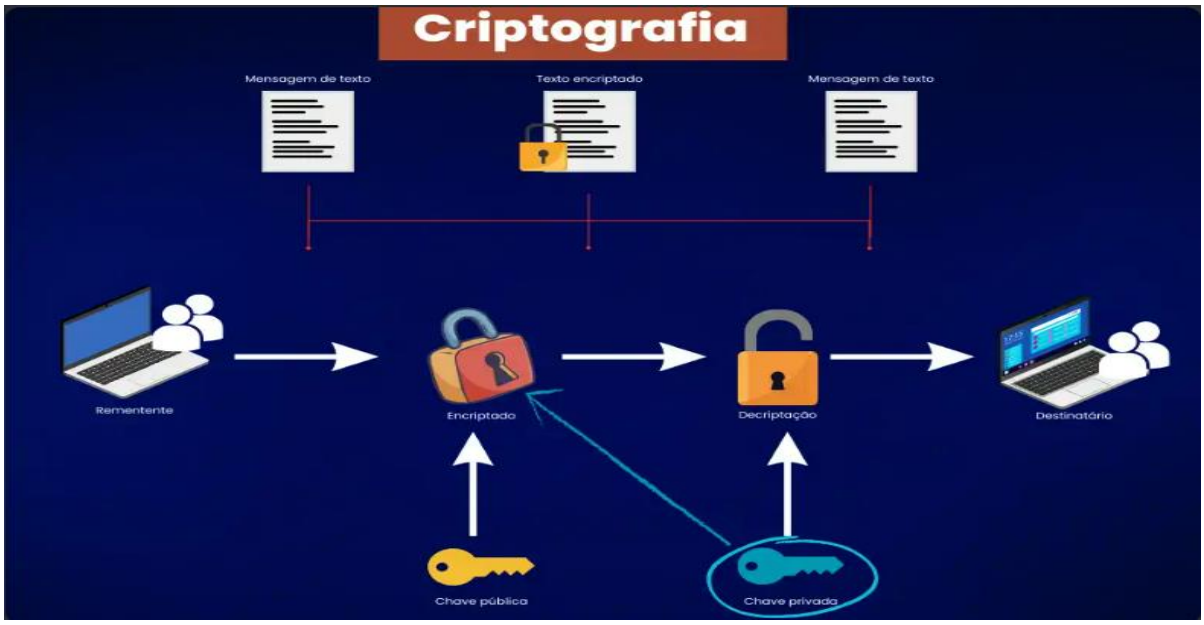
4. Engenharia social: Os cibercriminosos muitas vezes utilizam técnicas de engenharia social, como e-mails de *phishing* ou downloads maliciosos, para infectar os sistemas das vítimas.
5. Evolução constante: O *Ransomware* evoluiu ao longo dos anos para incluir variantes mais sofisticadas, que permite a indivíduos menos técnicos criar suas próprias campanhas de *Ransomware*.
6. Alvos variados: O *Ransomware* pode visar uma ampla gama de alvos, desde computadores pessoais até redes empresariais e até mesmo dispositivos IoT (Internet das Coisas).
7. Consequências graves: O *Ransomware* pode causar danos significativos, resultando em perda de dados, interrupção de operações empresariais e custos financeiros substanciais.

Após a infecção ser bem-sucedida, o *Ransomware* começa a criptografar arquivos e dados no sistema do computador da vítima. Usando algoritmos de criptografia, tornando impossível o acesso sem a chave correta (Santos, 2023).

Criptografia é a prática de codificar e decodificar dados. A partir do momento em que os dados são criptografados, um algoritmo é usado para codificá-los de forma que os usuários não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser restaurados ao seu formato original, usando uma chave descritiva especial (Liska, 2017), conforme mostra a Figura 2.

É importante ressaltar que a criptografia não é uma solução completa para a segurança de dados. Complementar a criptografia com boas práticas de segurança cibernética, como atualizações regulares de software, políticas de acesso restrito e conscientização sobre phishing, é essencial para uma defesa robusta contra ransomware e outras ameaças cibernéticas (Santos, 2023).

Figura 2 – Processo de criptografia de dados.



Fonte: Dio.me (2023).

A criptografia de dados é um tipo flexível de segurança. Pode ser aplicado a um dado específico, como uma única frase, ou mais amplamente a todos os dados de um documento ou mesmo a todos os dados contidos em mídias de armazenamento (Liska, 2017).

2.2 Leis e Normas

Está seção apresenta algumas leis relacionadas a segurança dos dados e algumas normas para a segurança da informação.

2.2.1 Lei Geral de Proteção de Dados (LGPD)

A LGPD, aprovada em agosto de 2018 e com o número 13.709, tem como principal objetivo proteger os dados de todo cidadão que esteja no Brasil. A lei tem a intenção de fornecer condições de segurança jurídica por meio da aplicação de padrões de regras e práticas (Serpro, 2018).

A lei dá ao cidadão uma série de proteções, incluindo a possibilidade de solicitar a exclusão dos seus dados pessoais, revogar o seu consentimento, transferir os seus dados para outro prestador de serviços, entre outras coisas. Alguns requisitos, como finalidade e necessidade, que devem ser já acordados e comunicados ao titular dos dados (Serpro, 2018).

Esta lei influenciou a criação *General Protection Regulation* (GDPR). Trata-se de uma lei que visa garantir a privacidade e o controle dos dados pessoais dos usuários nos países europeus e prevenir o uso indevido por terceiros (Fernandes, 2020).

Na Figura 3 estão ilustrados os principais pontos dessa lei. A norma estabelece ainda que a LGPD deve ser seguida se a sede da entidade estiver localizada em solo brasileiro ou no exterior, independentemente se as pessoas ali presentes são brasileiras ou não (Serpro, 2018).

Figura 3 – Os principais pontos da lei LGPD

Fonte: TecMundo (2021).

2.2.2 A norma ABNT NBR ISO 27005

A norma ABNT ISO 27005 fornece orientação para o gerenciamento de risco de SI em uma organização. Desta forma, cabe à organização especificar a sua abordagem, por exemplo no âmbito da gestão de riscos e do setor de atividade económica. Este padrão é baseado em método de identificação de riscos, ameaças e vulnerabilidades que não é mais atribuído pela ABNT NBR ISSO/IEC 27002 (ABNT, 2019).

De acordo com as consequências para o negócio e a probabilidade de ocorrência, as atividades de gerenciamento de riscos identificam as informações necessárias para identificação e avaliação de riscos (ABNT NBR ISO/IEC 27005, 2019).

2.3 Trabalhos Relacionados

Esta seção apresenta alguns trabalhos relacionados ao tema em estudo.

2.3.1 *Ransomware* e Cibersegurança: A informação ameaçada por ataques a dados

Protti (2020) abordou a modalidade de sequestro de dados na Internet conhecido como *ransomware,* investigando a possibilidade de ser criada uma regulação jurídica suficiente para tentar mitigar esse crime.

Realizou-se uma pesquisa bibliográfica visando definir os prejuízos das empresas em relação ao sequestro de dados através do crime de *ransomware*.

Foi concluído que, muitas das empresas que são atacadas não hesitam em fornecer o pagamento solicitado pelos criminosos, pois consideram que a perda dos dados levaria a prejuízos maiores do que o valor solicitado pelos criminosos.

2.3.2 As vulnerabilidades dos dados e as formas de ataques

O trabalho de Carneiro (2021) teve como objetivo identificar e descrever as formas de ataques aos dados mais conhecidas, apresentando os principais pontos de vulnerabilidades de acesso.

Através do estudo realizado, conclui-se que conhecer as formas de ataques e as correspondentes vulnerabilidades é uma das maneiras mais eficazes de se proteger as organizações desses ataques, além de utilizar *firewalls* e antivírus, criando assim, barreiras que podem deixar o ambiente empresarial mais seguro.

2.3.3 *Ransomware*: Segurança da informação e prevenção

O trabalho de Morais (2021) teve como objetivo apresentar as normas ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005, mostrando como exemplo um ataque de *ransomware*, além de sugerir maneiras de como um usuário pode se prevenir para garantir a segurança dos dados de seu computador.

Os resultados mostraram como atacar um computador, usando o sistema operacional Kali Linux, por meio da ferramenta *The Fat Rat*, listando um passo a passo para criar um *ransomware*, como exemplo de como atacar um computador pessoal.

Foi possível concluir que as políticas de segurança da ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005 tem como por princípios básicos a integridade, confidencialidade, disponibilidade de cada informação. E que aplicando as diretrizes destas normas corretamente podem tornar as redes mais seguras contra os ataques cibernéticos.

3 MÉTODO

De acordo com a sua natureza, este estudo é um resumo do assunto, procurando explicar a área de compreensão do projeto, indicando seu desenvolvimento histórico como consequência da investigação das informações obtidas e levando à compreensão de suas causas e explicações (Wazlawick, 2014).

De acordo com o objetivo, trata-se de um estudo exploratório e descritivo. Os métodos descritivos buscam dados mais consistentes sobre um determinado assunto, mas simplesmente apresentam os fatos como são, sem interferência dos pesquisadores (Wazlawick, 2014). Os estudos descritivos explicam as características de um determinado fenômeno ou população. Você também pode elaborar para identificar relacionamentos entre variáveis (Gil, 2017).

Muitas vezes, a pesquisa exploratória é considerada a primeira etapa do processo de pesquisa, pois o autor não precisa necessariamente ter um objetivo ou hipótese pré-determinada (Wazlawick, 2014).

Quanto aos procedimentos técnicos esta pesquisa é bibliográfica. A pesquisa bibliográfica foi elaborada a partir de materiais já publicados, como livros, teses, materiais encontrados na Internet, revistas, entre outros. O principal benefício é permitir um maior seguimento dos fenômenos do que seria possível investigar diretamente (Gil, 2017).

Segundo Gil (2017), as seguintes etapas são importantes para que a pesquisa bibliográfica se desenvolva:

a) A escolha de um tema: é preciso estar conectado aos interesses do aluno. Além disso, o conhecimento prévio sobre a área de estudo é necessário para que as fases subsequentes sejam bem desenvolvidas.

b) Levantamento bibliográfico preliminar: conforme o tema - Vulnerabilidade em redes de computadores corporativas: foram buscados estudos

de caso sobre ataques de *ransomware,* pesquisa de TCCs, artigos e livros sobre este tema.

c) Formulação do problema: - **Quais são os principais riscos de segurança em redes corporativas e como se proteger contra os ataques de *ransomware* em redes corporativas?**

e) Busca das fontes: busca nas bases de dados dos periodicos da capes visando responder o problema proposto, buscando as fontes bibliográficas capazes de fornecer informações, consultando dissertações, revistas científicas, obras de referência, outros materiais, entre outros.

f) Leitura do material: encontrar as informações e dados no material adquirido, estabelecendo conexões com o problema proposto e avaliando a coerência das informações e dados fornecidos pelos autores.

g) Fichamento: foi realizado para identificar as obras consultadas, anotar as ideias que surgiram, encontrar informações pertinentes, registrar os comentários feitos sobre as obras e organizar as informações apreendidas.

i) Redação do texto: escrita do Trabalho de Conclusão de Curso (TCC).

4 TIPOS DE ATAQUES E VULNERABILIDADES

Este capítulo apresenta os principais tipos de *ransomwares* e as vulnerabilidades que este ataque busca explorar. A abordagem do estudo relacionado as variantes dos ataques de *Ransomware* que serão citadas mais na frente, foram escolhidas devido os seguintes critérios: Variantes que mais receberam evoluções nos últimos anos, são consideradas as mais efetivas segundo seu propósito e lidarem com tratamento de dados sensíveis para as empresas ou dados de usuários comuns.

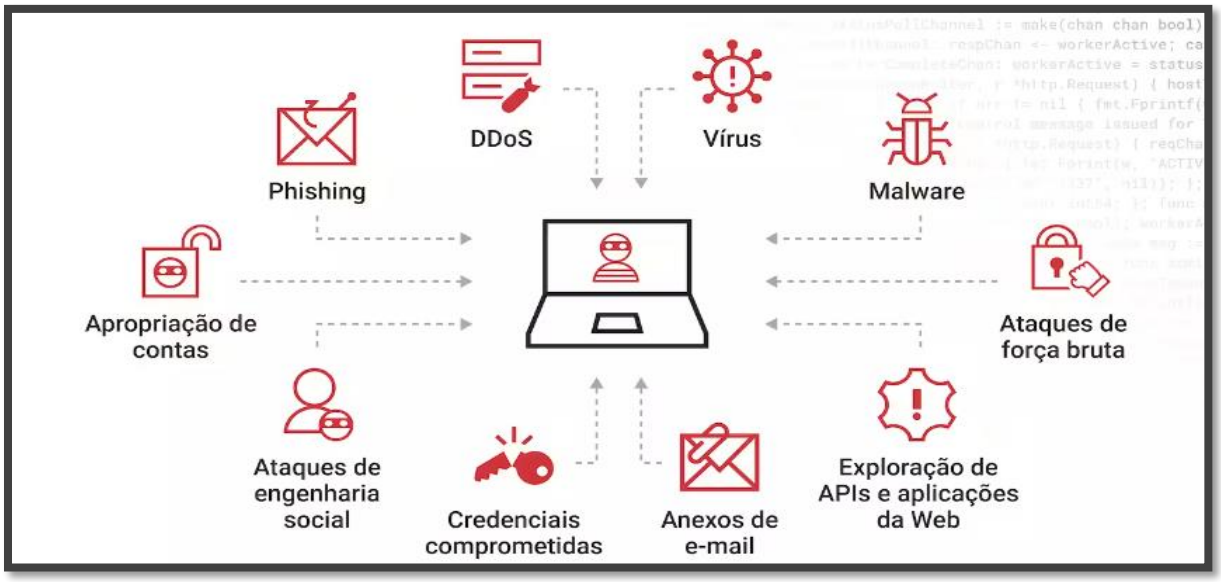
“Embora existam inúmeras variedades de *ransomware*, elas se enquadram em duas categorias principais” (Moura, 2022, p.21).

O objetivo do ***Crypto Ransomware*** é criptografar os arquivos valiosos da vítima como vídeos, documentos e fotos, tornando-os inúteis. Por exemplo, a funcionalidade do dispositivo não é afetada e os arquivos parecem ainda estar armazenados no sistema, mas não podem ser acessados (Moura, 2022).

Diferente do Crypto *ransomware*, o ***Ransomware Locker*** não criptografa arquivos. Em vez disso, destina-se a desativar funções básicas do dispositivo, como impedir parcialmente o uso do teclado ou dificultar o acesso à área de trabalho.

A Figura 4 mostra os alguns tipos de ataques mais comuns sofridos pelas empresas.

Figura 4 – Tipos de ataques mais comuns sofridos pelas empresas.



Fonte: Microsoft

4.1 *Scareware*

O *scareware* é um *malware* que infecta o sistema ou os dispositivos e então se apresenta como um alarme, alegando ter descoberto um vírus ou operação inadequada da máquina. Nesse caso, ele pede ao usuário que pague por um serviço falso que se compromete a corrigir o problema. Ou seja, é um tipo de ataque que se aproveita do medo do usuário para que consiga ter acesso ao sistema da vítima (Nakano, 2022).

Scareware é um tipo de ataque cibernético que os *hackers* usam para induzir as pessoas a baixarem o *malware*, clicar em links perigosos ou visitar sites infectados. O *scareware* tem o potencial de ser relativamente inofensivo e apenas atrapalhar a sua experiência de navegação, mas também tem o potencial de infectar seu dispositivo com *malware* e cause danos reais (Nakano, 2022). A Figura 5 apresenta um tipo comum de notificação nos ataques de *scareware*.

Figura 5 – Exemplo do tipo de notificação vista em ataques de *scareware.*

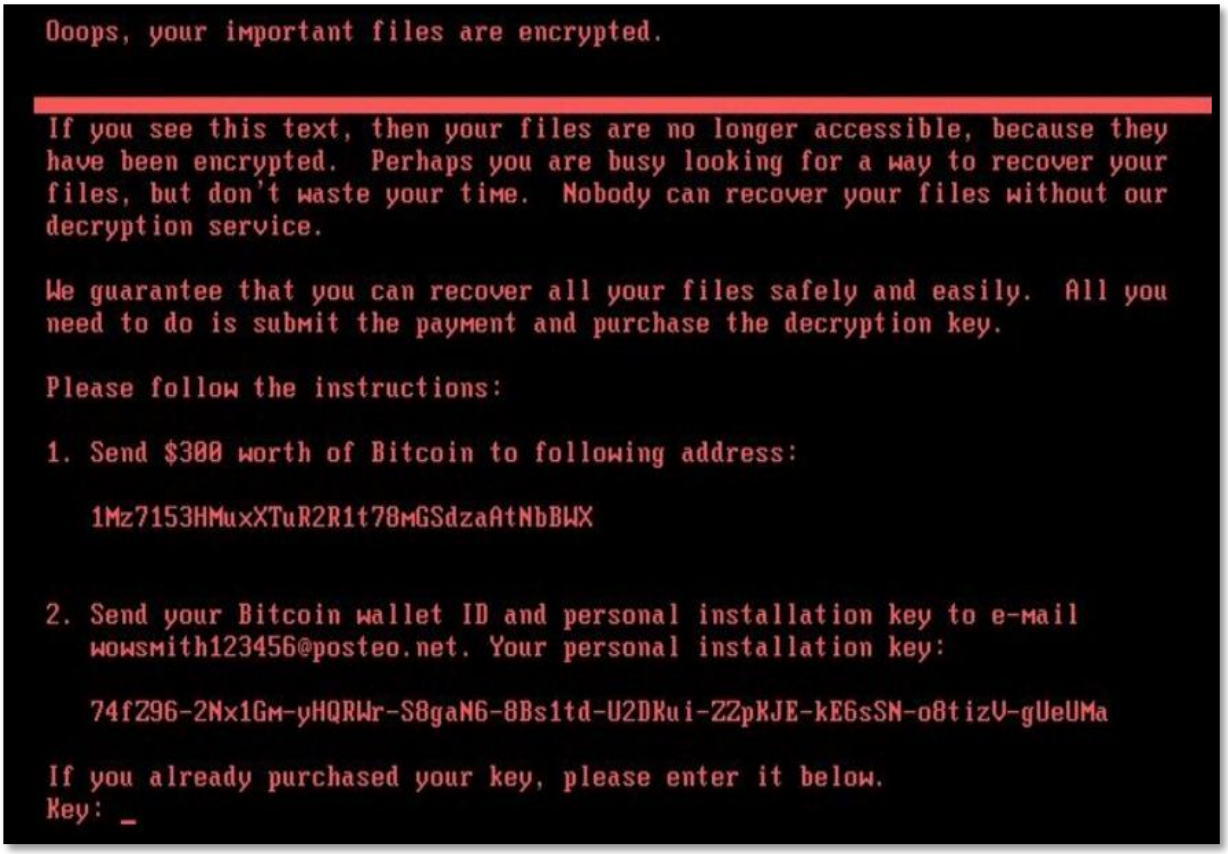
Fonte: Avast (2021).

4.2 *Petya*

Com grande poder de ação, *Petya* não só consegue acessar os documentos do usuário, como também criptografar todo o disco rígido do seu dispositivo. No processo de ataque, os cibercriminosos criptografaram a Tabela Mestre de Arquivos, impossibilitando completamente o acesso aos dados do disco (Clara, 2021).

Normalmente, o *Petya* conta com a ingenuidade dos usuários para ter acesso aos computadores. O usuário abre o e-mail malicioso, baixa o anexo, abre e concorda em fornecer permissões administrativas para alterar o sistema operacional. Somente quando esse processo for concluído, é capaz de começar a criptografar os dados. Em seguida, o computador da vítima é reiniciado e exibido uma mensagem de resgate, conforme mostrada na Figura 6 (Belcic, 2019).

Figura 6 – Mensagem do *Petya* informando que os dados foram criptografados.



Fonte: Avast (2019).

4.3 *Doxware*

Este *malware* se infiltra no sistema e ameaça expor os dados privadas e confidenciais para terceiros ou distribuí-las na rede. Devido esses dados serem mais valiosos para as empresas. Elas acabam sendo as vítimas mais visadas, uma vez que o vazamento é mais prejudicial do que o prejuízo financeiro (Nakamo, 2022).

O *Doxware* pode ser usado para atacar indivíduos e grandes organizações, para as quais tem sido frequentemente utilizado no passado. Esse tipo ataque pode envolver o roubo de fotos, vídeos, conversas ou credenciais de login, o que pode representar sérios problemas para a vítima se tornado público (Ress, 2023).

4.4 *Cerber*

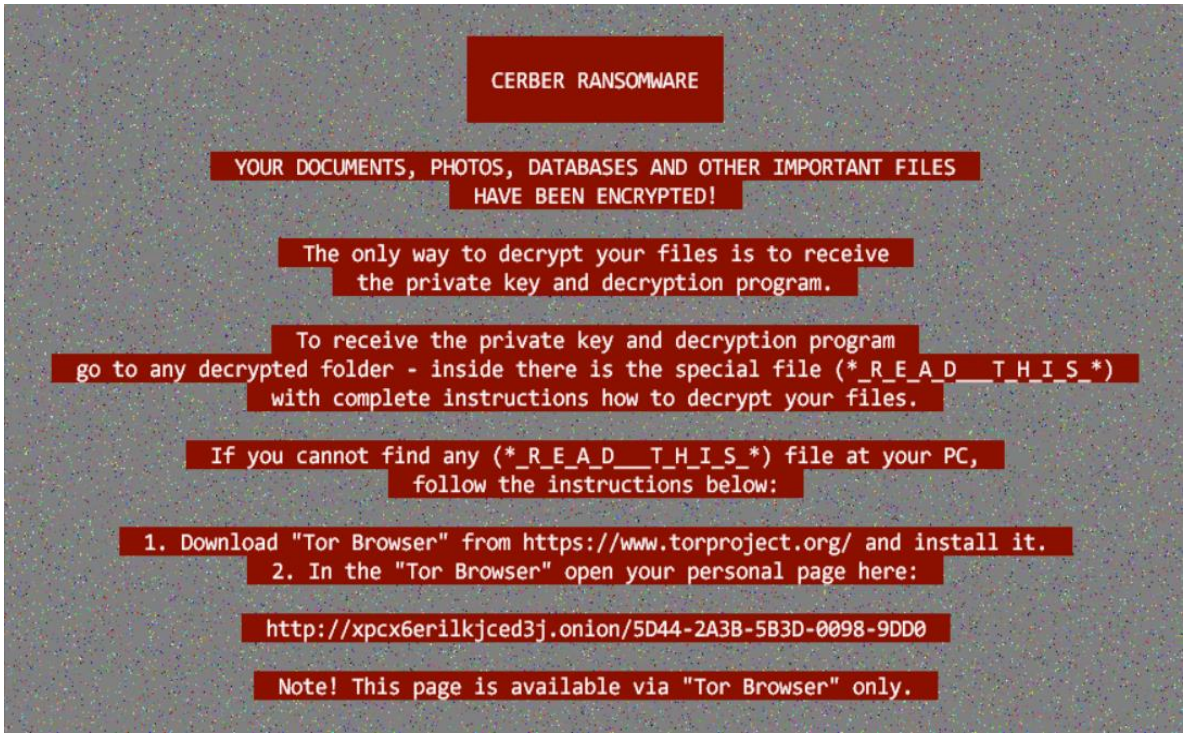
O *Cerber* é particularmente agressivo, pois suporta 12 idiomas diferentes. Essa versatilidade permitiu que seus criadores desenvolvessem “sistemas afiliados” como plataformas de *ransomware* como um serviço que traz lucros exorbitantes. O *malware* implanta campanhas de *phishing* elaboradas e visa principalmente usuários do *Office*

365 baseados em nuvem. Até agora, o *Cerber* atingiu milhares de vítimas (Clara, 2021).

O programa *Cerber* é bastante básico em termos de *ransomware*. Como consequência de e-mails de *phishing*, sites maliciosos ou anúncios exibidos em sites legítimos, as vítimas baixam o malware involuntariamente em seus dispositivos. Ao acessar um site malicioso, abrir um anexo malicioso ou interagir com um anúncio contaminado, o usuário pode acidentalmente instalar o *Cerber* no seu computador (Belcic, 2020).

Após instalado no computador do usuário, o *Cerber* inicia o processo de criptografia de seus dados para que o usuário não consiga mais abri-los. Depois que o *Cerber* concluir o processo de criptografia, será exibida uma mensagem de resgate explicando como será o método de pagamento proposto pelos criminosos, conforme apresentada na Figura 7 (Belcic, 2020).

Figura 7 – Exemplo de mensagem exibida pelo *Cerber*



Fonte: Avast (2019).

Segue a seguir a tradução para português da Figura 7:

“CERBER RANSOMARE

SEUS DOCUMENTOS, FOTOS, BANCOS DE DADOS E OUTROS ARQUIVOS IMPORTANTES FORAM CRIPTOGRAFADOS!

A única maneira de descriptografar seus arquivos é receber a chave privada e o programa de descriptografia.

Para receber a chave privada e o programa de descriptografia

vá para qualquer pasta descriptografada

- Dentro está o arquivo especial LEIA ISTO*)

com instruções completas sobre como descriptografar seus arquivos.

Se você não conseguir encontrar nenhum (*LEIA ISTO*) no seu PC,

siga as instruções abaixo:

1. Baixe o "Navegador Tor" em https://www.torproject.org/ e instale-o.

2. No "Navegador Tor, abra sua página pessoal aqui:

http://xpcx6erilkjced3J.onion/SD44-2A3B-5B3D-0098-9DDB

Observação! Esta página está disponível apenas através do Navegador Tor.”

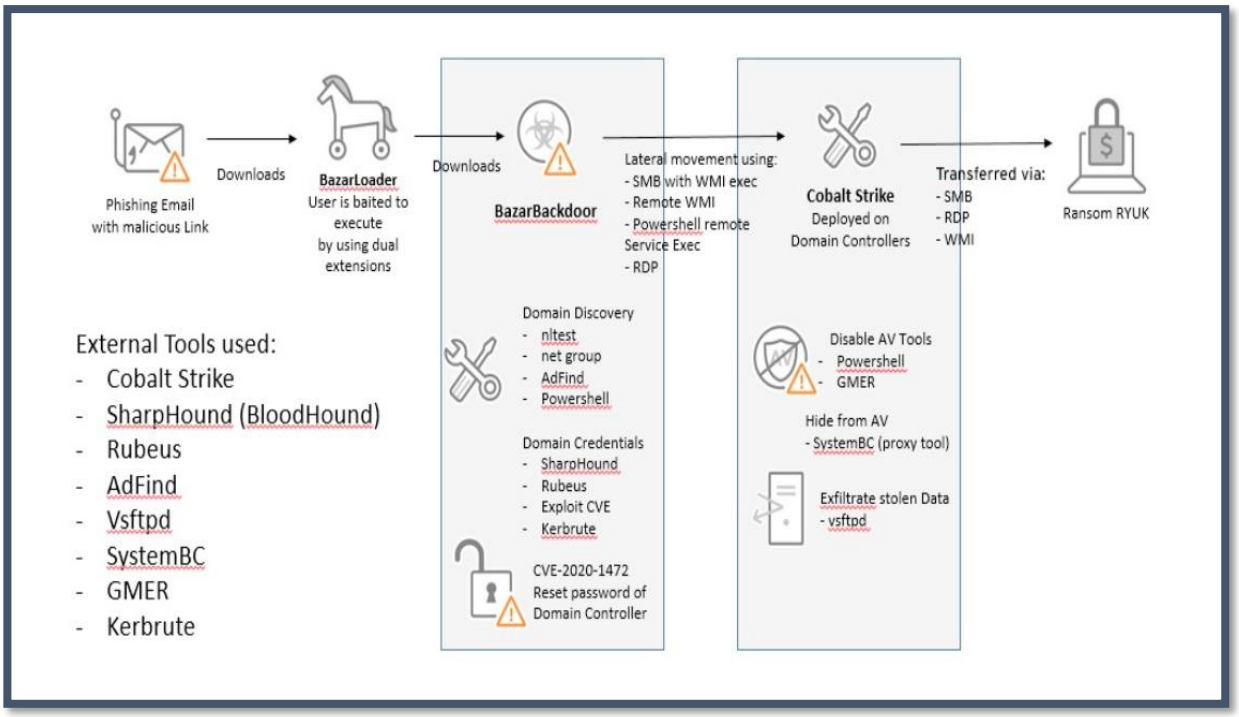
4.5 *Ryuk*

O *Ryuk* é uma das mais recentes variedades de *ransomware*. Com grande destaque em 2020, estima-se que mais de um terço de todos os ataques de *ransomware* naquele ano foram causados por este *malware*. Esta variante criptografa arquivos críticos para os negócios e exige resgates muito altos (geralmente na casa dos milhões). Alvos comuns para *Ryuk* são organizações, hospitais e agências governamentais (Clara, 2021).

Assim como os outros tipos de *Ransomware,* o *Ryuk* criptografa documentos, dados e sistemas de acesso a computadores, impossibilitando a recuperação de informações ou o acesso a programas. Ele também desativa a opção de restauração do sistema operacional *Windows*, obrigando as vítimas a escolher entre perder seus dados ou pagar a taxa. O ataque é tão cruel e devastador que muitos decidem pagar o resgate, tornando-o um dos ataques de *ransomware* mais lucrativo nos últimos anos (Burdova, 2022).

Por se tratar de uma ação efetuada pelo homem, os cibercriminosos por trás do *Ryuk* ficaram concentrados em utilizar as técnicas de engenharia social para a realização deste ataque, como golpes de *phishing, spams* e falsificação de sites, conforme mostrado na Figura 8 (Burdova, 2022).

Figura 8 – Ilustração de um ataque por meio de engenharia social



Fonte: TRENDmicro (2022).

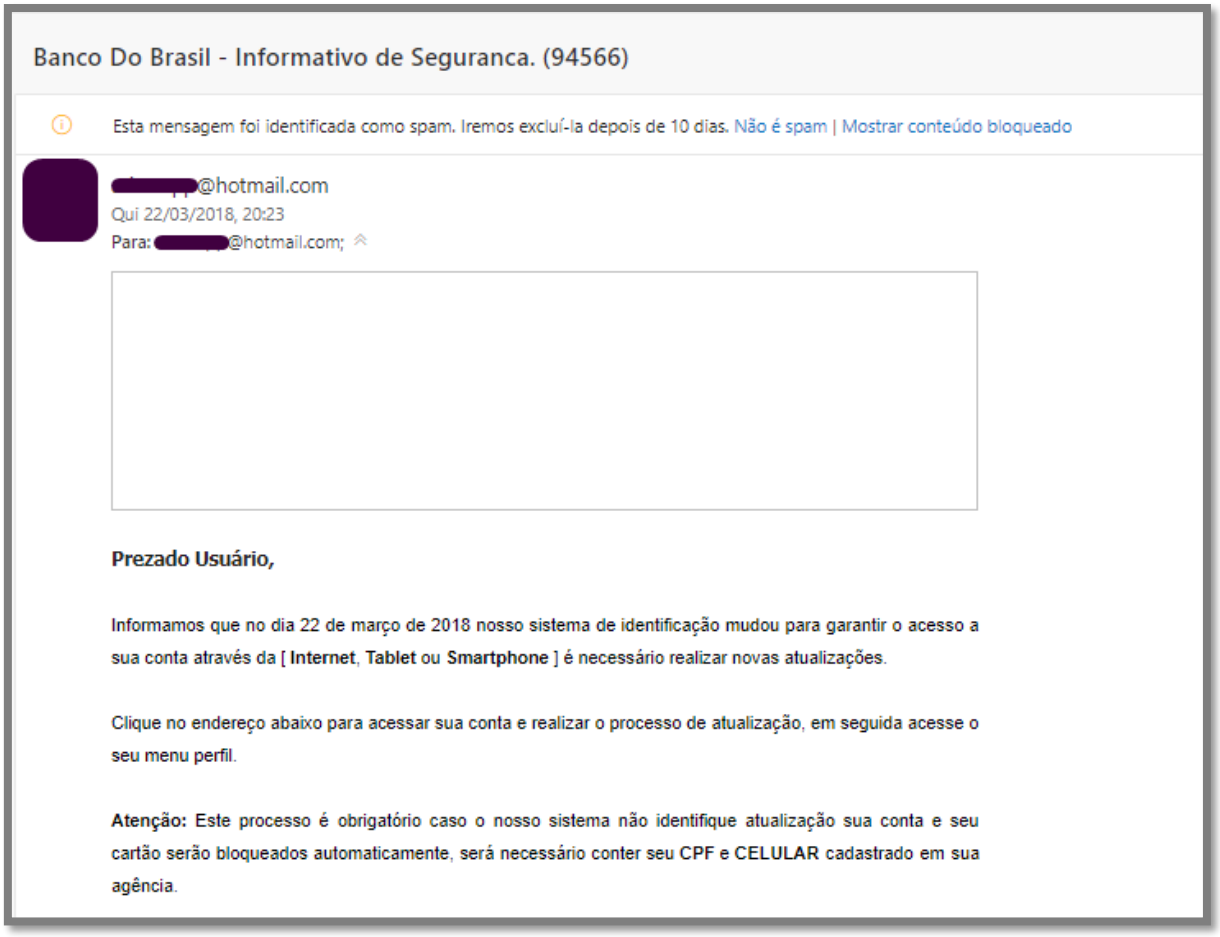
4.7 *Phishing*

Phishing é um tipo de crime cibernético no qual os criminosos fingem ser membros de uma organização legítima para induzir as vítimas a fornecer informações pessoais. Os *hackers* costumam entrar em contato com seus alvos por e-mail, telefone ou SMS, muitas vezes usando estratégias de comunicação e identidades visuais que combinam com o estilo de empresas conhecidas (Ariane, 2023).

Algumas informações sobre as empresas e os seus funcionários estão disponíveis nas redes sociais, como nome, local de trabalho, hábitos, entre outras informações. Dessa forma, redes sociais como *Facebook*, *Amazon*, *Netflix*, *Apple* e *WhatsApp* foram as redes que mais foram usadas em ataques de *phishing* em 2020, conforme ilustrado na Figura 2 (Zimmer, 2020).

No exemplo mostrado na Figura 9, o criminoso se faz passar por banco e os cabeçalhos dos e-mails já apresentam indícios de fraude. Os remetentes e destinatários são mascarados, indicando que o titular da conta enviou e recebeu o e-mail ao mesmo tempo (Ariane, 2023).

Figura 9 – Exemplo de um ataque *Phishing*



Fonte: Ariane (2023).

Segundo Stivani (2018), conhecer ataques de *phishing* em conjunto com programas antivírus é uma forma de prevenir possíveis ataques. Portanto, alguns dos ataques mais usados incluem:

- E-mails ou mensagens falsas: enviam e-mails ou mensagens que pareçam ser de uma empresa genuína. Se as vítimas não souberem que estão sendo enganadas, elas podem coletar informações clicando em links e inserindo dados. Os aplicativos executados incluem Dropbox e Google Docs;
- *Whaling* ou "Peixe Grande": Geralmente usados para entrar em contato com empresas, tentando primeiro entrar em contato com funcionários com altos cargos para obter acesso aos seus e-mails. Em seguida, solicita informações dos funcionários por meio de mensagens enviadas. Um invasor pode usar esta

mensagem ao responder a um administrador para obter informações confidenciais de sua organização;

- *Pharming*: Responsável principalmente por ataques a servidores DNS corporativos. Os invasores instalam cavalos de Tróia diretamente em uma rede ou computador host. Dessa forma, um endereço de site aparentemente seguro pode levar a um site falso e coletar informações de vários usuários ao mesmo tempo;
- *Vishing:* Um telefone é usado para enviar mensagens automáticas para vários números que dizem ser de uma empresa, na tentativa de induzir as vítimas a compartilharem informações pessoais.

Sistemas de segurança como *firewalls* e antivírus podem ajudar a tornar o ambiente corporativo mais seguro. No entanto, devido à falta de conhecimento sobre segurança cibernética entre os funcionários, o ambiente de negócios fica exposto a esses ataques. O treinamento para informar os funcionários sobre as políticas de segurança e as melhores práticas é, portanto, tão importante quanto proteger os sistemas (Zimmer, 2020).

5 FORMAS DE COMO PROTEGER AS REDES DE COMPUTADORES

Neste capítulo, serão apresentadas algumas estratégias essenciais que são consideradas necessárias para garantir a segurança das redes de computadores corporativas, abordando diversas medidas de proteção.

5.1 Criptografia dos dados

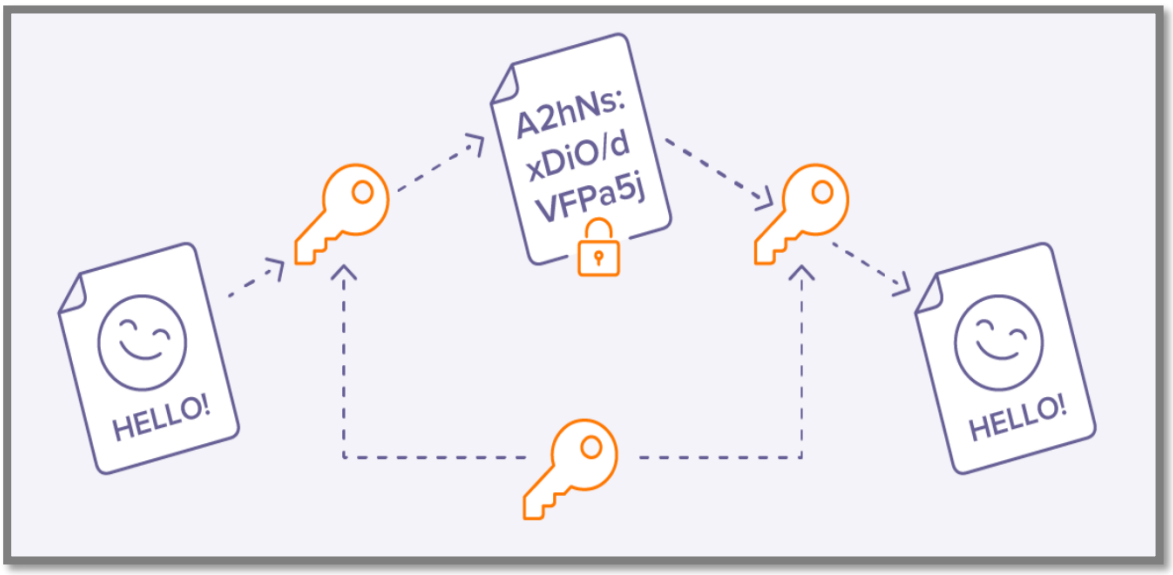
A Criptografia de Dados consiste em ser uma técnica ou estratégia para proteger a integridade das informações que são transmitidas e armazenadas em sistemas de redes de computadores. Esta técnica tem como principal objetivo permitir que apenas pessoas autorizadas possam acessar e compreender esses dados, sejam eles dados de empresas corporativas ou de uma simples rede particular (DeWitt, 2022).

A Criptografia é um processo que transforma informações de forma legível em um formato inelegível, que é chamado de texto cifrado, usando algoritmos matemáticos e chaves específicas (DeWitt, 2022).

O processo a seguir, mostra de forma mais detalhada como funciona a encriptação dessas informações:

- **Texto Claro:** O processo começa com um texto simples, que são os dados originais que você deseja proteger. Isso pode ser qualquer coisa, desde um simples e-mail ou até informações em um banco de dados.
- **Algoritmo de Criptografia:** É um conjunto de regras e operações matemáticas que determinam como os dados serão transformados. Existem diversos algoritmos de criptografia disponíveis, cada um com suas próprias características e níveis de segurança.
- **Chave de Criptografia:** Uma chave é um valor secreto usado como entrada no algoritmo de criptografia. Esta chave é fundamental nesse processo, pois é ela que determina como os dados serão cifrados. Dito isto, existem dois tipos principais de criptografia em relação à chave:
- **Criptografia Simétrica:** Acontece quando a mesma chave é usada tanto para cifrar quanto para decifrar os dados. Isso significa que a pessoa que cifrou os dados deve compartilhar a chave com a pessoa que deseja decifrá-los, conforme ilustrado na figura 10.

Figura 10 – Demonstração do funcionamento da Criptografia Simétrica.

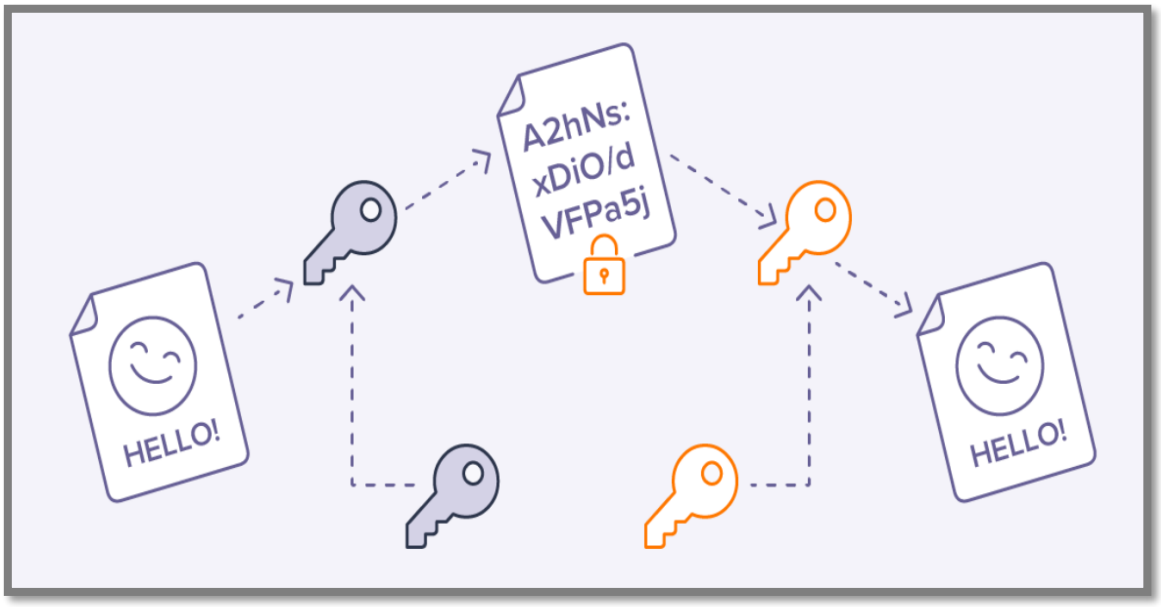


Fonte: Avast

- **Criptografia Assimétrica:** É considera mais segura, justamente pelo fato de um par de chaves, uma chave pública, que é usada para cifrar dados, e uma chave privada, que é mantida em segredo e usada para decifrar os dados. Isso

permite que qualquer pessoa cifre dados usando a chave pública, mas apenas a pessoa com a chave privada correspondente pode decifrá-los, como é mostrado na Figura 11.

Figura 11 – Como funciona Criptografia Assimétrica.



Fonte: Avast

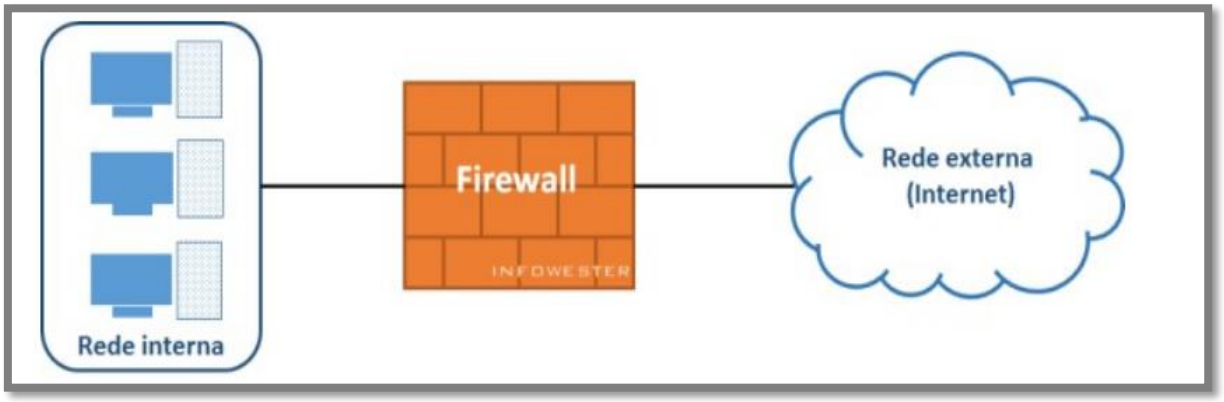
- **Cifragem:** O algoritmo de criptografia processa o texto de texto claro e a chave de chave para produzir o texto cifrado. O texto cifrado é a representação dos dados originais, mas é ilegível sem a chave de decifração apropriada.
- **Texto Cifrado (Texto Criptografado):** O texto cifrado é o resultado do processo de cifragem. Ele pode parecer uma sequência aleatória de números, letras e símbolos, mas é justamente uma representação codificada dos dados originais.
- **Transmissão ou Armazenamento Seguro:** O texto criptografado pode ser transmitido pela internet ou armazenado em dispositivos de forma segura. Mesmo se alguém interceptar o texto cifrado, ele não conseguirá compreendê-lo sem a chave de decifração adequada.
- **Decifração:** A pessoa ou sistema autorizado que possui a chave de decifração apropriada usa essa chave junto com um algoritmo de decifração compatível para reverter o processo de cifração. Isso resulta na recuperação dos dados originais, ou seja, tendo de volta o texto claro.

Com base nessas informações nota-se o quanto a criptografia pode ser eficaz e essencial para garantir a confidencialidade e a segurança das informações em um mundo digital onde os dados são constantemente transmitidos e armazenados em diversos dispositivos e sistemas.

5.2 *Firewall*

Um *Firewall* é um componente de segurança de rede ou *software* que atua como uma barreira entre uma rede privada ou dispositivo e a Internet ou outras redes não confiáveis, como é mostrado na Figura 12. O *firewall* tem como principal objetivo controlar o tráfego de rede, bloqueando ou permitindo o acesso com base em regras de segurança predefinidas. Com isso ele acaba desempenhando um papel significativo na proteção de sistemas e dados de redes de computadores corporativas ou privadas contra ameaças cibernéticas, como *hackers*, *malwares* e ataques de rede (Kovacs, 2021).

Figura 12 – Representação básica de um *firewall.*



Fonte: *Infowester*

Existem dois tipos principais de *firewalls* e ambos são projetados para proteger redes e sistemas de diferentes maneiras, porém cada um possui características distintas (Lima, 2022).

Firewall* de *Hardware:

É um dispositivo físico dedicado que geralmente é instalado entre a rede interna de uma organização e a Internet. Atuando como um ponto de controle central para rodo o tráfego de entrada e saída, permitindo que administradores definam regras para filtrar e inspecionar o tráfego de informações (Lima, 2022).

Firewalls de hardware geralmente oferecem um desempenho robusto, pois são construídos com *hardware* dedicado, processadores poderosos e recursos otimizados para lidar com grandes volumes de tráfego de rede. Esses *firewalls* são fisicamente isolados da rede que protegem, tornando mais difícil para invasores comprometerem o dispositivo (Pizzolato, 2022).

Firewall* de *Software:

É um programa ou aplicativo que é instalado em um dispositivo, como computador ou servidor. Ele age como uma barreira de proteção local para o dispositivo no qual está instalado e pode ser configurado para controlar quais aplicativos e serviços têm acesso à rede e à Internet (Lima, 2022).

Firewalls de *software* geralmente têm limitações de desempenho em comparação com firewalls de *hardware* dedicados. Isso ocorre porque eles são executados em servidores ou dispositivos de computação padrão, que podem não ter a mesma capacidade de processamento e recursos de *hardware* dedicado. Consequentemente, os *firewalls* de *software* podem não ser tão eficientes em lidar com grandes volumes de tráfego de rede ou ataques de alta intensidade (Pizzolato, 2022).

5.3 Antivírus e *Antimalware*

Na maior parte do tempo, ambos significam a mesma coisa. Pois são *softwares* projetados para proteger computadores e dispositivos eletrônicos contra ameaças cibernéticas, especialmente vírus de computador. Eles desempenham um papel fundamental na segurança da informação e na proteção da integridade e confidencialidade dos dados. Os vírus são programas maliciosos que se anexam a outros arquivos ou programas e se replicam quando esses arquivos ou programas são executados (Bar, 2019).

Os antivírus funcionam por meio de vários métodos para identificar e lidar com ameaças cibernéticas. Dentre eles então:

Análise de Assinaturas

A análise de assinaturas é um dos métodos fundamentais usados pelos antivírus para identificar e detectar ameaças cibernéticas. Essa técnica é baseada na comparação de padrões ou assinaturas conhecidas de *malware* com arquivos e

programas presentes no sistema. Ou seja, o antivírus compara arquivos e programas em seu sistema com uma base de dados de assinaturas conhecidas de vírus. Se houver uma correspondência, o arquivo é identificado como uma ameaça e é tratado de acordo (Bombonato, 2022).

De forma mais detalhada, a Análise de assinaturas segue os seguintes passos:

1. Criação de assinaturas

Os especialistas em segurança cibernética, laboratórios de segurança e empresas de antivírus monitoram constantemente a atividade da Internet em busca de novas ameaças.

Quando uma nova ameaça é identificada, eles analisam seu código para criar uma "assinatura" exclusiva que representa a ameaça.

A assinatura é geralmente uma sequência específica de *bytes* que é única para aquele *malware* em particular.

2. Compilação de Banco de Dados de Assinaturas

As assinaturas identificadas são armazenadas em um banco de dados de assinaturas.

Este banco de dados é atualizado regularmente para incluir novas ameaças à medida que são descobertas.

3. Varredura e comparação

Quando é executa uma verificação de antivírus no sistema, o *software* começa a varredura examinando arquivos e programas em busca de padrões que correspondam às assinaturas conhecidas de *malware*.

Isso geralmente envolve uma varredura minuciosa de arquivos no disco rígido, memória RAM e outros locais onde o *malware* pode estar escondido.

4. Identificação de Correspondências

Se durante a varredura o antivírus encontra um arquivo que possui uma correspondência exata com uma assinatura conhecida de *malware*, ele identifica esse arquivo como uma ameaça.

A identificação precisa de uma correspondência para evitar falsos positivos (identificação incorreta de arquivos legítimos como ameaças).

5. Ação sobre ameaças

Após identificar uma ameaça, o antivírus toma medidas para proteger o sistema. Isso pode incluir a quarentena do arquivo, a exclusão do arquivo ou a tentativa de reparar o arquivo, dependendo da configuração do antivírus e do impacto da ameaça.

A análise de assinaturas se destaca positivamente por ser rápida e eficaz na identificação de malwares conhecidos, e por uma taxa muito baixa de falsos positivos. Ou seja, quando bem ajustado conseguem identificar com precisão as ameaças (Bombonato, 2022).

Por outro lado, a análise de assinaturas depende da atualização regular da base de dados de assinaturas para proteger contra novas ameaças. *Malwares* novos e desconhecidos podem passar despercebidos até que uma assinatura seja criada (Bombonato, 2022).

Heurísticas

A heurística é uma técnica usada por programas antivírus e outros tipos de *software* de segurança cibernética para identificar ameaças com base em comportamentos suspeitos em vez de depender exclusivamente de assinaturas de *malware* conhecidas. É uma abordagem mais dinâmica para a detecção de ameaças e é projetada para lidar com *malwares* desconhecidos ou variantes de *malwares* existentes que foram modificadas para evitar a detecção por meio de análise de assinaturas (Nascimento, 2019).

A heurística examina o comportamento de programas e arquivos em execução no sistema em busca de atividades suspeitas. Isso pode incluir a monitoração de ações como a modificação de arquivos críticos do sistema, tentativas de se infiltrar em processos do sistema ou de outros programas, e atividades incomuns de rede (Magalhães, 2019).

Através da heurística o *software* de segurança cibernética define uma série de parâmetros e regras que determinam o que é considerado comportamento suspeito. Por exemplo, se um programa tentar modificar vários arquivos do sistema em uma

única operação, isso pode ser considerado suspeito. Com base nos parâmetros definidos, o *software* atribui uma pontuação de suspeita a atividades ou programas em execução. Quanto maior a pontuação, mais suspeita é a atividade (Magalhães, 2019).

Se uma atividade ou programa alcança uma pontuação de suspeita acima de um limite predefinido, o *software* de segurança pode tomar medidas, como bloquear a atividade, colocar o programa em quarentena ou notificar o usuário. A heurística consegue ser bastante eficaz na detecção de malwares desconhecidos ou variantes de *malwares* existentes que ainda não têm assinaturas conhecidas. Em relação a abordagem de Análise de Assinaturas, a heurística é mais flexível, pois não depende de atualizações de banco de dados de assinaturas (Andrade, 2022).

A heurística é uma ferramenta valiosa na luta contra as ameaças cibernéticas, especialmente aquelas que estão em constante evolução. Inclusive, para obter a melhor proteção possível, os programas de segurança cibernética geralmente combinam a heurística com outras técnicas de detecção, como análise de assinaturas, análise comportamental e análise de reputação, para oferecer uma proteção mais abrangente contra ameaças cibernéticas (Andrade, 2022).

Proteção em Tempo Real

A proteção em tempo real é uma característica fundamental dos programas antivírus e de segurança cibernética que monitoram constantemente a atividade do sistema em busca de ameaças em tempo real. Essa funcionalidade é essencial para identificar e responder rapidamente a ameaças cibernéticas assim que elas surgem.

Durante o monitoramento, o *software* de segurança avalia o comportamento de programas e processos em execução. Ele procura por atividades suspeitas, como tentativas de modificar arquivos críticos do sistema, acesso a sites maliciosos ou comportamento de rede anômalo (Nascimento, 2019).

Se o *software* de segurança identificar qualquer atividade que corresponda a um padrão de ameaça conhecido ou que atinja um nível de suspeita predefinido, ele tomará medidas imediatas para bloquear a ameaça ou notificar o usuário. A proteção em tempo real é considerada uma parte vital da defesa cibernética, ajudando a manter os sistemas protegidos contra ameaças em constante evolução. É importante escolher um *software* de segurança confiável e manter as definições

atualizadas para garantir que a proteção em tempo real funcione corretamente (Belcic, 2020).

5.4 *Backup* regular

O *backup* regular é uma prática fundamental nas empresas para garantir a segurança e a recuperação de dados em caso de perda, seja devido a falhas técnicas, erros humanos ou ataques cibernéticos, como *ransomware*. As empresas devem adotar medidas adicionais de segurança cibernética, como a implementação de *firewalls*, atualizações de *software*, treinamento de funcionários em conscientização de segurança e políticas de acesso para minimizar as chances de um ataque de *ransomware* bem-sucedido (Euripedes, 2023).

As empresas podem implementar uma rotina de *backup*, definindo quais dados e sistemas críticos devem ser copiados regularmente para locais seguros, como servidores dedicados ou serviços de armazenamento em nuvem. Esses *backups* podem ser agendados para serem feitos diariamente, semanalmente ou de acordo com a necessidade da empresa. Se uma empresa for vítima de um ataque de *ransomware*, em que os arquivos são criptografados e os criminosos exigem um resgate para descriptografá-los, os *backups* podem ser usados para restaurar os sistemas e os dados afetados, eliminando a necessidade de pagar o resgate (Santos, 2023).

Ter *backups* disponíveis para recuperação imediata pode reduzir o tempo de inatividade da empresa após um ataque, ajudando a retomar as operações mais rapidamente (Euripedes, 2023).

5.5 Monitoramento de Rede

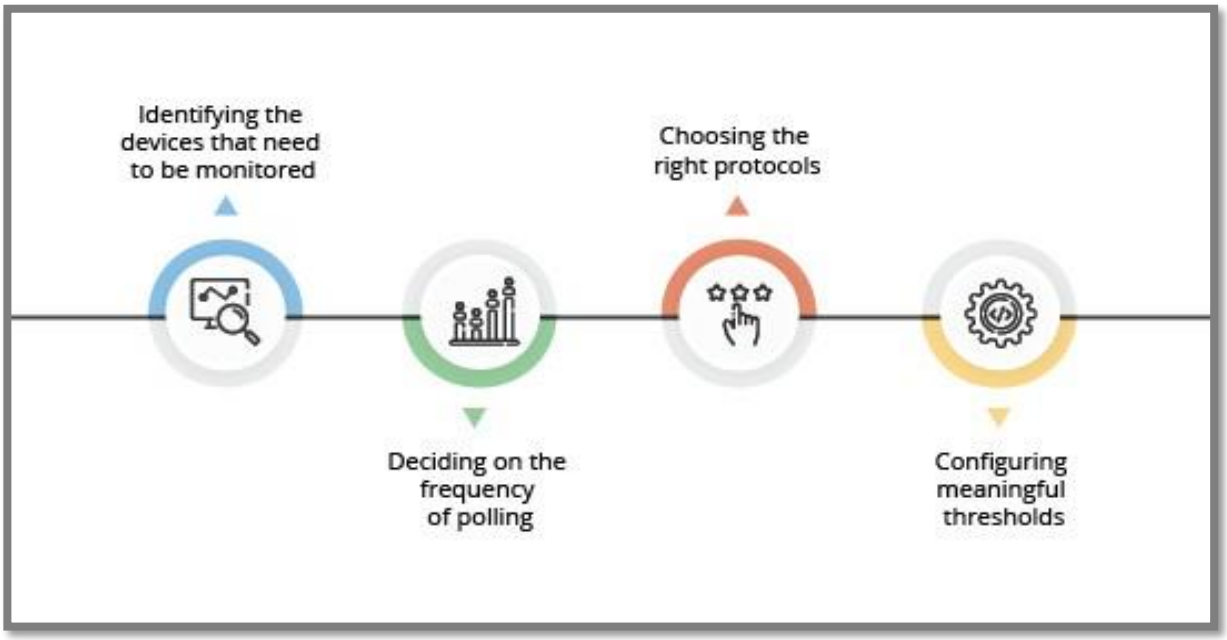
O monitoramento de rede é o processo de observar e analisar o tráfego de dados em uma rede de computadores para garantir que ela esteja funcionando de forma eficiente, segura e confiável. Ele desempenha um papel crucial na segurança e na administração de redes de computadores. Este processo coleta informações sobre o tráfego nos dispositivos da rede, e, em seguida, usa essas informações para tomar decisões informadas, identifica problemas e garante que a rede fique operando de acordo com as expectativas (Algar, 2022).

O termo monitoramento está relacionado a uma atividade de constante verificação, com o auxílio de dados. Portanto, o monitoramento de rede envolve a utilização de painéis, gráficos e relatórios que auxiliam na visualização e compreensão do que está ocorrendo. O principal objetivo é obter uma visão mais abrangente e precisa do que está acontecendo. Dessa forma, a empresa pode tomar decisões conscientes e seguras para otimizar as operações diárias (Tebaldi, 2022).

O processo de monitoramento de rede é considerado um ponto crucial na área de TI, justamente pelo fato de todos os componentes da rede, tais como roteadores, firewalls, servidores e Máquinas Virtuais (VMs), serem constantemente avaliados, aumentando o desempenho e diminuindo as falhas na rede. Esse processo encontra problemas de desempenho e gargalos no início, ajudando a identificar problemas no estágio inicial (Duarte, 2019).

A figura 13 ilustra os aspectos principais do monitoramento de rede, que são identificar os dispositivos que precisam ser monitorados, decidir a frequência de votação, escolher os protocolos certos e configurar os limites significativos.

Figura 13 – Aspectos principais do monitoramento de rede



Fonte: Como Aprender Windows

Segundo Julio (2020), esta abordagem apresenta diversas vantagens quando se trata da integridade em redes de computadores, tais como:

- **Detecção de Problemas:** A monitorização da rede auxilia na deteção de questões relacionadas com o desempenho, falhas de *hardware*, congestionamento do tráfego e outros problemas que possam ter impacto na operação da rede. Esse recurso permite que a equipe de TI adote medidas proativas para evitar interrupções.
- **Segurança:** O monitoramento da rede desempenha um papel crucial na proteção da segurança da rede. Ele tem a capacidade de identificar atividades maliciosas, como invasões, *malware* e ataques de negação de serviço (DDoS). Ao detectar ameaças em um estágio inicial, as equipes de segurança podem agir com maior rapidez e reduzir o impacto causado por incidentes de segurança.
- **Análise de Tráfego:** A monitorização da rede permite examinar o fluxo de dados em tempo real. Isso é extremamente importante para detectar comportamentos estranhos ou suspeitos que possam indicar uma violação de segurança. Além disso, contribui para otimizar a utilização da largura de banda e dos recursos da rede.
- **Conformidade:** Para inúmeras empresas, especialmente aquelas que gerenciam informações sensíveis, o monitoramento da rede é essencial para atender aos requisitos de conformidade regulatória. Regulamentações como o PCI-DSS ou Padrão de Segurança de Dados do Setor de Cartões de Pagamento, exigem monitoramento contínuo da rede para proteger as informações dos cartões de pagamento.
- **Planejamento e escalabilidade:** O monitoramento da rede entrega informações valiosas sobre a utilização desta rede ao decorrer do tempo. Isso permite que as empresas possam planejar expansões, atualizações e alocações de recursos de forma mais eficaz.
- **Resposta a Incidentes:** Em casos de incidentes de segurança, o monitoramento da rede desempenha um papel crucial na investigação e resolução. Os acessos de tráfego de rede podem ser usados para entender como um ataque aconteceu e o que foi comprometido.
- **Notificação antecipada:** Sistemas de monitoramento eficazes são capazes de fornecer avisos antecipados sobre possíveis problemas, permitindo que a

equipe de TI tome medidas antes que esses problemas tenham um impacto significativo nos usuários da rede.

- **Histórico e Auditoria:** O histórico apresentado pelo registro contínuo do tráfego de rede é útil para análises pós-incidentes e auditorias. Podendo ajudar na identificação de anomalias e na melhoria contínua da segurança da rede.

A manutenção da segurança das redes de computadores é fundamentalmente dependente do monitoramento da rede. Esse processo fornece dados essenciais para considerar e minimizar riscos à segurança, além de garantir que uma rede opere de forma eficiente e esteja em conformidade com as normas e padrões pertinentes (Cabral, 2019).

5.6 Atualizações de *Software*

As atualizações de *software* são modificações feitas em um programa de computador, aplicativo ou sistema operacional para melhorar, corrigir problemas, adicionar recursos, aprimorar o desempenho ou, em muitos casos, atualizar a segurança. Elas são lançadas periodicamente pelos desenvolvedores de *software* com o objetivo de manter o *software* relevante e funcional ao longo do tempo (Gofix, 2023).

As atualizações de *software* são essenciais para manter a funcionalidade, segurança e eficiência de aplicativos e sistemas. É recomendável que os usuários e empresas mantenham seus *softwares* atualizados para garantir que estejam protegidos contra ameaças cibernéticas, funcionando sem problemas e obtendo os benefícios dos recursos mais recentes. Geralmente, as atualizações podem ser aplicadas automaticamente, mas os usuários também podem optar por instalá-las manualmente (Ferreira, 2021).

De acordo com Gazola (2020), existem vários tipos de atualizações de *software*, e as principais são:

- **Atualizações de Segurança:** Essas atualizações são projetadas para corrigir vulnerabilidades de segurança no *software*. As vulnerabilidades são brechas que podem ser exploradas por *hackers* para comprometer a integridade de um sistema ou roubar informações. Manter o *software* atualizado com as últimas

correções de segurança é fundamental para proteger contra ameaças cibernéticas.

- **Atualizações de Correção de *Bugs*:** As atualizações de correção de *bugs* são lançadas para resolver problemas ou defeitos identificados no *software*. Isso pode incluir problemas de estabilidade, travamentos, erros de programação ou problemas de usabilidade.
- **Atualizações de Desempenho:** Essas atualizações visam melhorar o desempenho do *software*, tornando-o mais rápido, eficiente e responsivo. Isso pode envolver otimizações de código, redução do uso de recursos do sistema e aprimoramentos no funcionamento geral.
- **Atualizações de Recursos:** As atualizações de recursos adicionam novas funcionalidades ao software. Elas podem incluir novas ferramentas, opções de personalização, integração com serviços externos, aprimoramentos na interface do usuário e muito mais.
- **Atualizações de Compatibilidade:** À medida que sistemas operacionais e hardware evoluem, o *software* precisa ser atualizado para garantir que continue funcionando corretamente em novas plataformas e ambientes. Isso envolve manter a compatibilidade com sistemas operacionais mais recentes e *hardware* atualizado.

As atualizações de *software* de segurança são fundamentais para manter a integridade das operações de uma empresa, proteger seus ativos e dados, cumprir regulamentações, minimizar riscos financeiros e garantir a confiança dos clientes. Ignorar as atualizações de segurança coloca a empresa em risco de ataques cibernéticos. Portanto, é essencial que as empresas tenham políticas de gerenciamento de atualizações de segurança (Harada, 2020).

5.7 Filtragem de E-mails

A filtragem de e-mails é um processo pelo qual os e-mails recebidos são avaliados e classificados com base em critérios específicos. O objetivo é separar e-mails indesejados, como spam e *phishing*, dos e-mails legítimos e desejados. A filtragem de e-mails é usada para melhorar a eficiência da caixa de entrada, proteger contra ameaças de segurança e garantir que os usuários recebam apenas as mensagens relevantes (Gaidargi, 2018).

O e-mail corporativo é um serviço de e-mail utilizado por empresas e organizações para fins comerciais e de comunicação interna e externa. É uma forma de comunicação eletrônica profissional que permite que funcionários, executivos e outros membros da organização troquem mensagens, documentos e informações de maneira eficiente e segura (Lucciani, 2021).

A filtragem de e-mail ajuda a proteger as empresas contra ameaças cibernéticas, como *phishing*, *malware*, *ransomware* e vírus. Muitos ataques cibernéticos começam por meio de e-mails maliciosos. Os filtros de e-mail identificam e bloqueiam mensagens suspeitas, ajudando a evitar que funcionários cliquem em links maliciosos ou abram anexos perigosos (Flood, 2021).

De acordo com Fraga (2019) o processo de filtragem de mails pode variar dependendo do *software* ou serviço que se está usando. Mas na maioria das vezes funciona da seguinte forma:

- Recebimento de E-mails: O processo começa quando o servidor de e-mails da sua organização ou provedor de e-mail recebe mensagens de e-mail de remetentes externos. Essas mensagens são direcionadas para as contas de e-mail dos destinatários.
- Análise de Cabeçalhos: O sistema de filtragem analisa os cabeçalhos de cada mensagem de e-mail. Isso inclui informações sobre o remetente, destinatário, servidores envolvidos e outros detalhes.
- 3. Análise de Conteúdo: O conteúdo do e-mail, incluindo o texto, imagens e anexos, é examinado em busca de elementos suspeitos, como palavras-chave associadas a *spam* ou *phishing*. Além disso, padrões e características que podem indicar uma mensagem maliciosa são verificados.
- Verificação de Anexos: Se houver anexos no e-mail, o sistema verifica esses anexos em busca de *malware* ou vírus. Anexos maliciosos podem ser identificados e tratados adequadamente.
- Listas de Bloqueio: O sistema verifica se o endereço IP do servidor de origem está listado em listas de bloqueio conhecidas. Se estiver listado em uma lista de bloqueio de servidores de *spam*, a mensagem pode ser bloqueada.

- Lista de Permissões: O sistema verifica se o remetente está na lista de permissões da organização. Se o remetente estiver na lista de permissões, a mensagem provavelmente passará sem ser filtrada.
- Pontuação de Spam: Cada e-mail é atribuído uma pontuação com base na análise de conteúdo, cabeçalhos e outros fatores. Essa pontuação é comparada a um limite predefinido. Se a pontuação for superior a esse limite, a mensagem pode ser classificada como spam.
- Autenticação de Remetente: As tecnologias de autenticação, como *Sender Policy Framework* (SPF) e *Domain Keys Identified Mail* (DKIM), são usadas para verificar a autenticidade do remetente. Isso ajuda a garantir que o e-mail realmente venha do domínio alegado no remetente.
- Ações de Filtragem: Com base na pontuação e na análise, o sistema de filtragem de e-mails toma ações apropriadas.
- *Feedback* do Usuário: Alguns sistemas de filtragem de e-mails permitem que os usuários classifiquem manualmente mensagens de spam ou legítimas. Essas classificações são usadas para melhorar os algoritmos de filtragem.

A filtragem de e-mails é uma combinação de tecnologia, regras de segurança, análise de conteúdo e políticas personalizadas que trabalham em conjunto para proteger as empresas contra ameaças cibernéticas e garantir o fluxo eficiente de comunicações eletrônicas (Gaidargi, 2018).

5.8 Políticas de segurança e aplicações de normas pelas empresas

A segurança cibernética é uma parte crítica dos negócios modernos. A implementação de mecanismos de segurança e a adesão a normas ajudam as empresas a proteger seus ativos, manter a continuidade das operações e demonstrar compromisso com a segurança da informação, o que é essencial em um mundo digital cada vez mais ameaçador (Harford, 2021).

A importância de mecanismos de segurança e aplicações de normas pelas empresas contra ataques cibernéticos é fundamental em nosso cenário atual. As ameaças cibernéticas estão se tornando cada vez mais complexas, sofisticadas, maliciosas, bem organizadas e bem financiadas (Narayanan 2021).

As normas de segurança cibernética e conformidade são essenciais para proteger a infraestrutura crítica. Segundo a Agência de Segurança da Infraestrutura e

Cibersegurança, a infraestrutura crítica descreve os sistemas físicos e cibernéticos e ativos que são tão vitais para os Estados Unidos que sua incapacidade ou destruição teria um impacto debilitante em nossa segurança física ou econômica ou saúde ou segurança pública (Wang, 2021).

De acordo com Harford (2021), as empresas podem adotar diversas políticas e normas de segurança. E algumas delas são ilustradas na figura 14 e mencionadas no texto a seguir:

Figura 14 – Instruções de como preparar uma empresa contra-ataques cibernéticos.

Fonte: Microsoft

- Plano de Recuperação: A primeira fase envolve a preparação de um plano de recuperação. Isso inclui dificultar o acesso e a interrupção de sistemas, bem como a criptografia ou a destruição de dados essenciais da organização. Além disso, facilitar a recuperação da organização após ataques sem pagar o resgate é crucial.
- Limitar o Escopo dos Danos: A segunda fase envolve limitar o escopo dos danos. Isso é feito dificultando o trabalho dos invasores de obter acesso a vários sistemas comercialmente críticos por meio de funções de acesso privilegiado.
- Dificultar a Entrada: A terceira fase envolve dificultar a entrada dos invasores. Isso é feito tornando o trabalho dos atacantes muito mais difícil enquanto eles tentam obter acesso às infraestruturas locais ou em nuvem.

- Treinamento de Usuários: O treinamento de usuários reduz bastante o risco de infecção. Os usuários podem ser treinados para identificar ameaças cibernéticas, incluindo *ransomware*, *phishing* e engenharia social.
- Manter o Software Atualizado: Certifique-se de que o *firmware*, as aplicações *antimalware*, os sistemas operacionais e o *software* de terceiros tenham o *patch* mais recente instalado. Novas versões de *ransomware* são lançadas regularmente e as atualizações de software garantem que seu antimalware reconheça ameaças mais recentes.
- *Backups* Regulares: A melhor maneira de se recuperar de um *ransomware* é restaurar os dados de um *backup*. Os backups contornam o pedido de resgate, restaurando os dados de uma fonte diferente dos arquivos criptografados.

As normas de segurança e a aplicação de políticas de segurança são essenciais para proteger a integridade, confidencialidade e disponibilidade dos ativos de informações de uma empresa. Elas ajudam a cumprir regulamentações, manter a continuidade dos negócios e preservar a confiança dos clientes, fatores críticos em um ambiente corporativo cada vez mais digital e sujeito a ameaças cibernéticas. Portanto, é essencial que as empresas implementem políticas de segurança e normas para proteger seus sistemas contra ataques de *Ransomware* (Feitosa, 2021).

5.9 Conscientização dos Funcionários

A conscientização dos funcionários é uma parte crucial das medidas de segurança cibernética em empresas corporativas. Funcionários bem informados e treinados desempenham um papel fundamental na prevenção de ataques cibernéticos e na proteção dos ativos de informações da empresa (Bertolli, 2022).

Treinar os funcionários em segurança cibernética é um investimento fundamental na proteção da empresa contra ameaças cibernéticas. Funcionários conscientes e bem treinados desempenham um papel crítico na prevenção de ataques, na manutenção da segurança dos dados e na proteção da reputação da empresa (Esposito, 2018).

Auxiliar os funcionários sobre segurança cibernética tem como objetivo não apenas explicar por que é importante falar sobre o tema, como também criar uma mudança cultural na empresa para que a cibersegurança seja uma prioridade na vida do funcionário até mesmo fora do ambiente de trabalho (Brayda, 2023).

A conscientização dos funcionários sobre segurança cibernética tem como objetivo explicar por que é importante falar sobre o tema e criar uma mudança cultural na empresa para que a cibersegurança seja uma prioridade na vida do funcionário, até mesmo fora do ambiente de trabalho. É nesta etapa que os funcionários entendem por que precisam ter senhas fortes ou prestar atenção a e-mails recebidos de fora da organização (Furtado, 2023).

Segundo estudo feito pela empresa Gartner (2023) até 2025, mais da metade dos ataques cibernéticos de grande escala serão resultado de falhas humanas. Um levantamento feito com 1.310 funcionários de empresas ao redor do mundo em maio de 2022 mostrou que 69% dos funcionários ignoraram ao menos uma orientação de cibersegurança no ambiente de trabalho nos 12 meses anteriores. Além disso, 74% deles disseram que ignorariam recomendações se isso os ajudasse a atingir seus objetivos de negócios.

A *Fortinet*, empresa especializada em segurança cibernética, divulgou o resumo de uma pesquisa realizada em 2023, destacando a importância de as empresas elaborarem mecanismos de conscientização dentro do ambiente de trabalho, fortalecendo assim a segurança e reduzindo os ataques online. A pesquisa mostrou que 81% das empresas sofreram ataques maliciosos e que foram direcionados, principalmente, aos funcionários.

De acordo com Bertolli (2022) os aspectos importantes relacionados à conscientização dos funcionários são:

- Treinamento e Educação: As empresas devem fornecer treinamento regular em segurança cibernética para todos os funcionários, independentemente do nível de conhecimento técnico. Isso inclui treinamento sobre como reconhecer ameaças cibernéticas, como *phishing*, *ransomware* e engenharia social.
- Políticas e Procedimentos: Funcionários devem estar cientes das políticas e procedimentos de segurança da empresa. Isso inclui o uso de senhas fortes, a política de uso de dispositivos pessoais, o relato de incidentes de segurança e outras diretrizes relevantes.
- Conscientização sobre *Phishing*: O treinamento de conscientização sobre *phishing* é fundamental, pois são uma das ameaças mais comuns. Os

funcionários devem aprender a identificar e relatar e-mails de *phishing* e mensagens suspeitas.

- Senhas Seguras: Os funcionários devem ser educados sobre a importância de senhas fortes e práticas de gerenciamento de senhas, como não compartilhar senhas e atualizá-las regularmente.
- Ameaças de Engenharia Social: Os funcionários devem ser instruídos sobre como reconhecer e evitar ameaças de engenharia social, como ligações telefônicas fraudulentas e solicitações de informações confidenciais.
- Acesso Seguro: Os colaboradores da empresa devem ser orientados sobre práticas seguras de acesso a sistemas e redes, incluindo autenticação de dois fatores e uso de VPNs quando necessário.
- Uso Seguro de Dispositivos Pessoais: Se a empresa permitir o uso de dispositivos pessoais no trabalho, os funcionários devem ser informados sobre as políticas de segurança relacionadas a esses dispositivos, como a instalação de *software* de segurança e atualizações regulares.
- Cultura de Segurança: Promover uma cultura de segurança é essencial. Cada colaborador deve entender que a segurança cibernética é responsabilidade de todos e que a conscientização é um esforço contínuo.
- Testes de Conscientização: As empresas podem realizar testes regulares de conscientização para avaliar o conhecimento e a prontidão dos funcionários em relação a ameaças cibernéticas.
- Comunicação e Atualizações: Manter uma comunicação constante e eficaz sobre questões de segurança cibernética é importante. Isso pode incluir a divulgação de alertas de segurança e atualizações regulares sobre novas ameaças e melhores práticas.

Embora não seja possível alcançar uma segurança cibernética perfeita, a combinação de medidas de segurança e treinamento dos funcionários é uma estratégia eficaz para reduzir riscos, proteger ativos e melhorar a postura de segurança da empresa. É importante entender que a segurança cibernética é um esforço contínuo que exige adaptação constante às ameaças em evolução (Furtado, 2023).

6 CONCLUSÃO

Este projeto teve o intuito de responder a seguinte questão de pesquisa: **- Quais são os principais riscos de segurança em redes corporativas e como se proteger contra os ataques de *ransomware* em redes corporativas?**

Este estudo permitiu identificar os principais riscos de segurança em redes corporativas, sendo: Ataques de *Ransomware,* Ataques de *Phishing*, *Sniffing*, Inadequação de Políticas de Segurança e Falta de conscientização e treinamento dos funcionários.

- Ataques de *Ransomware*: Pode se infiltrar na rede, criptografar os dados e exigir um pagamento para restaurá-los.
- Ataques de *Phishing*: manipula os funcionários das empresas, se passando por outra pessoa, seja um colega ou o supervisor, para obter dados confidenciais;
- *Sniffing*: *softwares sniffers* observam pacotes ou dados não criptografados em trânsito na rede;
- Inadequação de Políticas de Segurança: Políticas de segurança fracas ou até mesmo desatualizadas que podem deixar a rede vulnerável a ameaças.
- Falta de conscientização e treinamento dos funcionários: Funcionários desinformados ou sem treinamento algum sobre práticas de segurança podem abrir portas para possíveis invasores.

Os criminosos cibernéticos exploram vulnerabilidades nos sistemas, coletam dados dos funcionários e observam minuciosamente falhas na infraestrutura de rede da empresa. Essa abordagem lhes permite adquirir as informações essenciais para invadir o sistema corporativo, realizando o roubo de dados ou comprometendo o acesso às informações.

Com o estudo feito, concluiu-se que conhecer os tipos de ataques de *ransomware* e as correspondentes vulnerabilidades pode ser uma das melhores maneiras de prevenir as organizações desses crimes. Além disso, utilizar *firewalls* e antivírus, por exemplo, pode deixar o ambiente empresarial ainda mais seguro.

Além disso, os funcionários também representam uma vulnerabilidade para as empresas, expondo-as a ataques como o *phishing*. Tais ataques criam uma ilusão de que as comunicações provêm de fontes confiáveis ou manipulam os usuários para

obter informações valiosas, tanto das vítimas quanto das empresas. Portanto, o treinamento contínuo dos funcionários dentro da organização são ferramentas fundamentais para prevenir tais incidentes.

Assim, no contexto atual, é muito importante que as empresas implementem mecanismos de segurança e sigam normas para se protegerem contra ataques cibernéticos. As ameaças nesse campo estão se tornando mais complexas, sofisticadas e organizadas, aumentando a importância dessas medidas de proteção.

Embora, não exista uma solução única para prevenir todos os ataques e eliminar as vulnerabilidades de uma empresa, existem métodos eficazes de proteção e diretrizes recomendadas, como treinar os funcionários e implementar políticas de segurança consistentes em toda a organização. Conhecer os tipos de ataques frequentes e entender as táticas dos cibercriminosos também é fundamental para proteger a empresa contra ameaças cibernéticas.

Para continuidade deste trabalho, sugere-se as seguintes sugestões para trabalhos futuros:

- Fazer um estudo prático sobre algumas ferramentas de prevenção contra os ataques de *Ransomware*;
- Simular a criação de um ataque de *Ransomware* em uma rede de computadores;

REFERÊNCIAS

ALECRIM, Emerson. **O que é Tecnologia da Informação (TI)?**. Infowester. 2019. Disponível em: https://www.infowester.com/ti.php. Acesso em: 7 abr. 2023.

ALGAR, **O que é monitoramento de rede e veja 6 *softwares* recomendados.** Cnx. 2022. https://blog.algartelecom.com.br/tecnologia/monitoramento-de-rede/1/.Acesso em: 10 nov. 2023.

AMADO, Miguel. **Marco Civil da Internet: o que é, importância e mudanças propostas**. FIA. 2019. Disponível em: https://fia.com.br/blog/marco-civil-da-internet/.Acesso em: abr. 2023.

ANDRADE, M.D; BENTES, D.S; GUIMARÃES, D.F.S. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais**. Revista Vertentes do Direito**.** Tocantins, v. 4, n. 2, p. 191- 205, nov. 2017.

ARAUJO, Nonata. **Segurança da Informação**. Administradores. 2022. Disponível em: https://administradores.com.br/artigos/seguranca-da-informacao-ti Acesso em: 10 abr. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:** Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, ABNT, 2005.

BATISTA, Emerson. **Sistema de Informação: o uso consciente da tecnologia para o gerenciamento**. Saraiva. 2004. Disponível em: http://www.avm.edu.br/docpdf/monografias_publicadas/C204769.pdf Acesso em:abr. 2023.

BELCIC, Ivan. **O que é um sniffer e como se proteger contra ele?.** Avast. 2020. Disponível em: https://www.avast.com/pt-br/c-sniffer#topic-1. Acesso em: 02 maio 2023.

BELCIC, Ivan. ***Ransomware Petya*: Como funciona e como se proteger.** Avast. 2019. Disponível em: https://www.avast.com/pt-br/c-petya/. Acesso em: 12 nov. 2023. ***Ransomware Cerber*: Tudo que você precisa saber.** Avast. 2020. Disponível em: https://www.avast.com/pt-br/c-cerber/. Acesso em: 11 nov. 2023.

BERTOLLI, Emília. **Conscientiza sua organização sobre segurança cibernética.** Varonis. 2022. Disponível em: https://www.varonis.com/pt-br/blog/conscientize-sua-organizacao-sobre-seguranca-cibernetica/. Acesso em: 08 nov. 2023.

BOMBONATO, Bianca. **O que é um Antivírus de nova geração?** AvantServices. 2021. https://www.avantservices.com.br/2022/05/27/o-que-e-um-antivirus-de-nova-geracao/. Acesso em: 05 nov. 2023.

BRAYDA, Carlo. **12 dicas para proteger sua empresa contra ataques cibernéticos.** Forbes. 2023. Disponível em: https://forbes.com.br/forbes-tech/2023/07/12-dicas-para-proteger-sua-empresa-contra-ataques-ciberneticos/.Acesso em: 10 nov. 2023.

BRITO, Douglas. **Combatendo a ameaça ransomware aplicando a norma NBR ISO/IEC 27001:2013 na gestão da segurança da informação.** 2016.Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/19456/1/CT_GETIC_V_2015_07.pdf. Acesso em abr. 2023.

BURDOVA, Carly. **O que é o *Ransomware Ryuk*?.** Avast. 2022. Disponível em: https://www.avast.com/pt-br/c-ryuk-ransomware/. Acesso em: 11 nov. 2023.

BUXTON, Oliver. **O que é um *scareware*? Detecção, prevenção e remoção.** Avast. 2022. Disponível em: https://www.avast.com/pt-br/c-scareware/. Acesso em: 10 nov. 2023.

CLARA, Julio. **Tipos de Ransomware: Principais variações e métodos de ataque** Backup garantido. 2021. Disponível em: https://backupgarantido.com.br/blog/tipos-de-ransomware/. Acesso em: maio. 2023.

DEWITT, Derek. **Criptografia de dados: O que é?** Avast. 2021. Disponível em: https://www.avast.com/pt-br/c-encryption/. Acesso em: 04 out. 2023.

DUARTE, Leonardo. **O que é monitoramento de Rede?*.*** Como Aprender Windows. 2019. https://comoaprenderwindows.com.br/utilitarios/o-que-e-monitoramento-de-rede/. Acesso em: 10 nov. 2023.

DURBANO, Vinicius. **Segurança da Informação: o que é e 12 dicas práticas para garantir**. Ecoit. 2018. Disponível em: https://blog.ecoit.com.br/seguranca-da-informacao/.Acesso em: abr. 2023.

ESPOSITO, Jeffrey. **Como educar os funcionários sobre Cibersegurança?.** Kaspersky. 2018. Disponível em: https://www.kaspersky.com.br/blog/best-practices-for-workplace/11162/. Acesso em: 7 nov. 2023.

EURIPEDES, Victor. **Por que é importante fazer *Backups* de seus arquivos e dados?** Linkedin. 2023. https://www.linkedin.com/pulse/por-que-%C3%A9-importante-fazer-backups-de-seus-arquivos-e-l-s-/?originalSubdomain=pt. Acesso em: 03 nov. 2023.

FEITOSA, Alessandro. **Empresas vítimas de *Ransomware* precisam avisar sobre ataque? Quem investiga? Veja perguntas e respostas*.*** Globo.com. 2021. https://g1.globo.com/tecnologia/noticia/2021/09/28/empresas-vitimas-de-ransomware-precisam-avisar-sobre-ataque-quem-investiga-veja-perguntas-e-respostas.ghtml/. Acesso em: 02 nov. 2023.

FERNANDES, Mirian. **O que é *sniffer*? Como se proteger?**. Starti. 2021. Disponível em: https://blog.starti.com.br/sniffer/. Acesso em: maio 2023.

FERNANDES, Mirian. **Tudo sobre segurança cibernética**. Starti. 2020. Disponível em: https://blog.starti.com.br/tudo-sobre-seguranca-cibernetica/. Acesso em: abr. 2023.

FERREIRA, Thiago. **A importância de usar versões atualizadas de *Software.*** Medium. 2021. https://medium.com/whatsgooddev/a-import%C3%A2ncia-de-usar-vers%C3%B5es-atualizadas-de-software-ef744692a23a/. Acesso em: 02 nov. 2023.

FLOOD, Breandan. **Filtragens de E-mails*.*** Pipedrive. 2021. https://support.pipedrive.com/pt/article/email-filtering/. Acesso em: 02 nov. 2023.

FORTINET. **Comunicado à imprensa.** Fortinet. 2023. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2023/fortinet-research-finds-over-80-perfect-of-organizations-experience-cyber-attacks-that-target-employees. Acesso em: 08 nov. 2023.

FURTADO, Paul. **A importância da conscientização e treinamento de cibersegurança para funcionários.** Linkedin. 2023. Disponível em: https://www.linkedin.com/pulse/import%C3%A2ncia-da-conscientiza%C3%A7%C3%A3o-e-treinamento-de-ciberseguran%C3%A7a/?originalSubdomain=pt/. Acesso em: 10 nov. 2023.

GAIDARGI, Juliana. **A importância do e-mail corporativo*.*** Infonova. 2018. https://infonova.com.br/a-importancia-do-email-corporativo/#:~:text=Obter%20um%20bom%20sistema%20de,acabe%20na%20pasta%20de%20spam./. Acesso em: 02 nov. 2023.

GALOYAN, Albert. **Segurança Cibernética no Âmbito das Relações Internacionais**. 2019. Trabalho de Conclusão de Curso (Bacharel em Relações Internacionais) – Universidade de Brasília, Brasília, 2019.

GAZOLA, Rodrigo. **Dicas de segurança da informação: Por que manter os *Softwares* atualizados?*.*** Addee. 2020. https://addee.com.br/blog/softwares-atualizados/. Acesso em: 02 nov. 2023.

GOFIX. **Por que atualização regular de *Software* é importante?** Linkedin. 2023. https://www.linkedin.com/pulse/por-que-atualiza%C3%A7%C3%A3o-regular-de-softwares-%C3%A9-importante-gofix/?originalSubdomain=pt/. Acesso em: 02 nov. 2023.

GONÇALVES, Ariane. **O que é *phishing* e como se proteger de golpes na internet.** Hostinger. 2021. Disponível em: https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet#Como-se-proteger-de-ataquesphishing. Acesso em: maio 2023.

HARFORD, Isabella. **Tipos de controle de segurança cibernética e como colocá-los*.*** Tech Target. 2021. https://www.techtarget.com/searchsecurity/feature/Types-of-cybersecurity-controls-and-how-to-place-them/. Acesso em: 02 nov. 2023.

HASSAN, Nihad A. **Endpoint Defense Strategies.** In: HASSAN, Nihad A. **Ransomware Revealed**. Berkeley: Apress, 2019, p. 71-114.Disponível em: https://periodicos.uninove.br/thesisjuris/article/view/16739. Acesso em: maio 2023.

JULIO, Clara. **Monitoramento de rede: Importância, vantagens e melhores ferramentas*.*** Backup Garantido. 2020. https://backupgarantido.com.br/blog/monitoramento-de-rede/. Acesso em: 06 nov. 2023.

KOVACS, Leandro. **O que é um *Firewall*? E a diferença para um Antivírus.** Tecnoblog. 2021. Disponível em: https://tecnoblog.net/responde/o-que-e-um-firewall-e-a-diferenca-para-um-antivirus/. Acesso em: 12 out. 2023.

LARA. Rodrigo. **Ransomware: por que o sequestro de dados está bombando e como se defender.** Uol. 2022. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2022/06/09/ransomware-o-que-e-e-por-que-esta-na-modo-o-sequestro-de-dados-e-sistemas.htm.Acesso em: 10 abr. 2023.

LATTO, Nica. **O que é um *sniffer* e como não ser espionado?**. AVG. 2020. Disponível em: https://www.avg.com/pt/signal/what-is-sniffer. Acesso em: maio 2023.

LIMA, **Diferença entre *Firewall* de *Hardware* e *Firewall de Software*.** Acervo Lima. 2021. Disponível em: https://acervolima.com/diferenca-entre-firewall-de-hardware-e-firewall-de-software/. Acesso em: 10 out. 2023.

LISKA. A.; GALLO.T. **Ransomware Dedending Against Digital Extortion**. 2017.

LUCCIANI, Geraldo. **E-mail corporativo: o que é e como funciona?*.*** Blog task. 2021. https://blog.task.com.br/email-corporativo-o-que-e/. Acesso em: 02 nov. 2023.

LUCENA, Felipe. **Segurança de Dados: tudo que você precisa saber**. Diferencial TI. 2017. Disponível em: https://blog.diferencialti.com.br/seguranca-de-dados/. Acesso em: 06 abr. 2023.

MACÊDO, Diego. **Entendendo os *sniffers***. DiegoMacêdo. 2017. Disponível em: https://www.diegomacedo.com.br/entendendo-os-sniffers/#more-6462. Acesso em: 12 maio 2023.

MAGALHÃES, Thiago. **Antivírus de última geração com aprendizado de máquinas e inteligência artificial** Medium. 2019. https://medium.com/@thiagootcm/antiv%C3%ADrus-de-%C3%BAltima-gera%C3%A7%C3%A3o-com-aprendizado-de-m%C3%A1quinas-e-intelig%C3%AAncia-artificial-41acd368848f/. Acesso em: 07 nov. 2023.

MARTINS, Geiza. **O que é o Marco Civil da Internet?** Super Interessante. 2018. Disponível em: https://super.abril.com.br/mundo-estranho/o-que-e-o-marco-civil-da-internet/. Acesso em: abr. 2023.

MENEZES, Elizabeth. **Resumo de redes de Computadores para tribunais.** Estratégia Concursos. 2023. Disponível em: https://www.blogson.com.br/conceitos-de-redes-corporativas/.Acesso em: 08 abr. 2023.

MOREIRA, C.; BEIRA, J.C; OLIVEIRA, M. **Um olhar dos estudantes do curso de biblioteconomia acerca do que são dados, informações e conhecimentos**. Informação & Informação. Londrina, v. 25, n. 2, p. 484 – 508, abr./jun. 2020.

MOURA, Bianca. **Ransomware mais perigosos.** Psafe. 2022. Disponível em: https://www.psafe.com/blog/os-14-tipos-de-ransomware-mais-perigosos-da-web/. Acesso em: maio. 2023.

NAKANO, Alexandre. **Tipos de Ransomware: Quais são?** Ingrammicro. 2022. Disponível em: https://blog.ingrammicro.com.br/seguranca-da-informacao/tipos-de-ransomware/. Acesso em: maio. 2023.

NARAYANAN, Laskshmi. **Evolução das operações e estratégias de segurança para construir um SOC eficaz*.*** Isaca. 2021. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc/. Acesso em: 10 nov. 2023.

NEVES.A. **Como evitar se tornar uma vítima de ransomware?**. Samsung e Segurança. 2018. SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **O que muda com a LGPD**. Serpro. 2018.Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 03 abr. 2023.

NONES, Fernanda. **LGPD: o que diz a lei de proteção de dados e como ela pode impactar a sua estratégia de marketing e vendas**. Resultados Digitais. 2022. Disponível em: https://resultadosdigitais.com.br/marketing/o-que-e-lgpd/Acesso em: 16 abr 2023.

OLIVEIRA, Anderson. **Conceitos de Rede Corporativas.** Blogson. 2015. Disponível em: https://www.blogson.com.br/conceitos-de-redes-corporativas/.Acesso em: 08 abr. 2023.

OLIVEIRA, Natália. **O que é um banco de dados?.** Dev. 2020. Disponível em: https://dev.to/nfo94/o-que-e-um-banco-de-dados-56fm. Acesso em: maio. 2023.

PAYÃO, Felipe. **SQL Injection: saiba tudo sobre um ataque simples que pode ser devastador**. Tecmundo. 2017. Disponível em: https://www.tecmundo.com.br/tecmundo-explica/113195-sql-injection-saiba-tudo-ataque-simples-devastador.htm. Acesso em: 23 abr. 2023.

RAMOS, K.S.; SAPIA, H.M; ALESSI, H.C; ALESSI, R.M; RUIZ, G.A; FERRARI, D.J; PEREIRA, D.R. **Gestão de segurança da informação em uma empresa do setor de saúde: um estudo de caso**. *Colloquium Exactarum**.*** São Paulo, v. 9, n. 4, p. 33 – 40, abr. 2023.

RESENDE FILHO, Dirceu Moraes. **SQL Server – como evitar SQL injection?.** iMasters. 2019. Disponível em: https://imasters.com.br/banco-de-dados/sql-server-como-evitar-sql-injection. Acesso em: abr. 2023.

RESS, Katie. **O que é *Doxware*?.** Makeuseof. 2023. Disponível em: https://www.makeuseof.com/what-is-doxware/. Acesso em: 07 nov. 2023.

RODRIGUES, André. ***Sniffing* de rede**. Portal GSTI. 2019. Disponível em: https://www.portalgsti.com.br/2018/11/sniffing-de-rede.html. Acesso em: maio 2023.

SANTOS, Anderson. ***Ransomware:* Entendendo a ameaça que pode paralisar as empresas.** Dio.me. 2023. Disponível em: https://www.dio.me/articles/ransomware-enendendo-a-ameaca-que-pode-paralisar-empresas. Acesso em: 15 out. 2023.

SANTOS, Tiago. **Segurança da Informação: Protegendo o mundo digital contra ameaças de Vírus e *Malware.*** Dio.me. 2023. https://www.dio.me/articles/seguranca-da-informacao-protegendo-o-mundo-digital-contra-ameacas-de-virus-e-malware/. Acesso em: 06 nov. 2023.

SCHULTZ, Felix. **Segurança cibernética: o que é e como se tornar um especialista no assunto**. Milvus. 2023. Disponível em: https://blog.milvus.com.br/seguranca-cibernetica-o-que-e/#:~:text=%C3%89%20uma%20ramifica%C3%A7%C3%A3o%20da%20seguran%C3%A7a,e%20manipular%20dados%20ou%20arquivos.Acesso em: 14 abr. 2023.

SOUZA, Ivan De. **Banco de dados: saiba o que é, os tipos e a importância para o site da sua empresa**. Rockcontent. 2020. Disponível em: https://rockcontent.com/br/blog/banco-de-dados/. Acesso em: maio. 2023.

STIVANI, Mirella. **Os dez tipos de phishing mais comuns**. Techtudo. 2018. Disponível em: https://www.techtudo.com.br/listas/2018/06/os-dez-tipos-de-phishing-mais-comuns.ghtml. Acesso em: maio 2023.

TAVELLA, Fernando. ***Ransomware* Conti: Principais características e como funcionam seus afiliados.** WeLiveSecurity. 2021. Disponível em: https://www.welivesecurity.com/br/2021/12/09/ransomware-conti-principais-caracteristicas-e-como-funcionam-seus-afiliados/. Acesso em: 11 nov. 2023.

TOTUS. **Segurança de dados: por que é prioridade nas empresas?.** Totus. 2020. Disponível em: https://www.totvs.com/blog/negocios/seguranca-de-dados/.Acesso em: 14 abr. 2023.

VELOSO, Thássius. **O que é segurança da Informação?**. Tecnoblog. 2023. Disponível em: https://tecnoblog.net/responde/o-que-e-seguranca-da-informacao/Acesso em: 11 abr. 2023.

WONG, Caroline. **Por que as regulamentações e conformidade de segurança cibernética são tão importantes em nosso cenário atual de ameaças*.*** Forbes. 2021. https://www.forbes.com/sites/forbestechcouncil/2021/11/23/why-cybersecurity-regulations-and-compliance-are-so-important-in-our-current-threat-landscape/. Acesso em: 10 nov. 2023.

ZEFERINO, D. **Dados, informação e conhecimento: qual a diferença dos conceitos.** [Brasil] 12 ago. 2020. site Certifiquei. Acessado em: < https://www.certifiquei.com.br/dados-informacao-conhecimento/ >. Acessado em: abr. 2023.

ZIMMER, Kelvin. ***Hacker* x empresas: quais os ataques cibernéticos mais comuns?.** Lumiun Blog. 2020. Disponível em: https://www.lumiun.com/blog/hackers-empresas-quais-os-ataques-ciberneticos-mais-comuns/. Acesso em: 7 maio 2023.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 • Setor Universitário
Caixa Postal 86 • CEP 74605-010
Goiânia • Goiás • Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br • reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Marco Aurélio Sirqueira de Sá do Curso de Engenharia de Computação, matrícula 20182003300773, telefone: 62 98261-8078 e-mail masds100@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado VULNERABILIDADE EM REDES DE COMPUTADORES CORPORATIVAS: ESTUDOS DE CASOS SOBRE ATAQUES DE RANSOMWARE, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 12 de Setembro de 2023.

gov.br Documento assinado digitalmente
MARCO AURELIO SIRQUEIRA DE SA
Data: 11/09/2023 21:07:04-0300
Verifique em https://validar.iti.gov.br

Assinatura do autor: _____

Nome completo do autor: MARCO AURÉLIO SIRQUEIRA DE SÁ

Assinatura do professor–orientador: SOLANGE DA SILVA

Nome completo do professor-orientador: gov.br Documento assinado digitalmente
SOLANGE DA SILVA
Data: 13/09/2023 20:56:56-0300
Verifique em https://validar.iti.gov.br