INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
CAMPUS JOÃO PESSOA
DIRETORIA DE ENSINO SUPERIOR
UNIDADE ACADÊMICA CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

ERICK AMARO DUTRA DE LIMA

PRÁTICAS PARA MITIGAR ATAQUES CIBERNÉTICOS EM SISTEMAS DE TELECOMUNICAÇÕES: ESTUDO DE CASO

JOÃO PESSOA - PB
2024

ERICK AMARO DUTRA DE LIMA

PRÁTICAS PARA MITIGAR ATAQUES CIBERNÉTICOS EM SISTEMAS DE TELECOMUNICAÇÕES: ESTUDO DE CASO

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia da Paraíba como parte dos requisitos para obtenção do título de Tecnólogo em Sistemas de Telecomunicações.

Patric Lacouth da Silva
Orientador

JOÃO PESSOA - PB
2024

Dados Internacionais de Catalogação na Publicação – CIP
Biblioteca Nilo Peçanha –IFPB, *Campus* João Pessoa

L732p Lima, Erick Amaro Dutra de.
Práticas para mitigar ataques cibernéticos em sistemas de telecomunicações : estudo de caso / Erick Amaro Dutra de Lima. – 2024.
68 f. : il.

TCC (Graduação – Tecnologia em Sistemas de Telecomunicações) – Instituto Federal da Paraíba – IFPB / Coordenação de Tecnologia em Sistemas de Telecomunicações, 2024.
Orientação: Profº. Dr. Patric Lacouth da Silva.

1.Segurança cibernética. 2. Cibersegurança. 3. Segurança em redes. I. Título.

CDU 004.056:007(043)

Bibliotecária responsável Lucrecia Camilo de Lima – CRB15/132

ERICK AMARO DUTRA DE LIMA

PRÁTICAS PARA MITIGAR ATAQUES CIBERNÉTICOS EM SISTEMAS DE TELECOMUNICAÇÕES: ESTUDO DE CASO

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia da Paraíba como parte dos requisitos para obtenção do título de Tecnólogo em Sistemas de Telecomunicações.

Aprovada em 28 / 08 / 2024

Banca Examinadora

gov.br
Documento assinado digitalmente
PATRIC LACOUTH DA SILVA
Data: 14/10/2024 16:53:40-0300
Verifique em https://validar.iti.gov.br

Profº Dr. Patric Lacouth da Silva

Orientador

gov.br
Documento assinado digitalmente
GUSTAVO ARAUJO CAVALCANTE
Data: 14/10/2024 17:01:05-0300
Verifique em https://validar.iti.gov.br

Profº Dr. Gustavo Araújo Cavalcante
Examinador

gov.br
Documento assinado digitalmente
JULIO CEZAR DE CERQUEIRA VERAS
Data: 14/10/2024 18:33:55-0300
Verifique em https://validar.iti.gov.br

Profº Msc. Júlio Cezar de Cerqueiras Veras
Examinador

JOÃO PESSOA - PB
2024

AGRADECIMENTOS

É com imensa gratidão que inicio este momento de reconhecimento e agradecimento, pois a conclusão deste curso marca não apenas o término de uma etapa acadêmica, mas também o resultado de muitos esforços, superações e aprendizados ao longo desses anos.

Em primeiro lugar, expresso minha profunda gratidão a Deus, fonte da vida e razão de todas as conquistas. A Ele, agradeço pelo dom da vida e por todas as providências concedidas ao longo desta jornada acadêmica, Sua orientação e sustento foram fundamentais para que eu pudesse superar desafios.

À minha amada esposa, Mirleny, dedico um agradecimento especial. Pois, sua compreensão e apoio foram essenciais durante todo o período de estudos. Agradeço também por dedicar seu precioso tempo às nossas filhas Marina e Angelina enquanto eu estava presente nas aulas.

Não posso deixar de expressar minha sincera gratidão aos caríssimos professores que, com dedicação exemplar, compartilharam seus conhecimentos valiosos. Além das aulas, suas brincadeiras, conselhos e boas risadas tornaram a jornada acadêmica não apenas educativa, mas também enriquecedora em experiências humanas.

Aos amigos que caminharam ao meu lado durante esses longos anos, meu mais profundo agradecimento. Foram muitas as conversas, compartilhamento de informações diversas e as boas risadas, isto fez desta trajetória acadêmica uma sem dúvidas uma experiência marcante.

Dedico, assim, esta conclusão de curso a todos que contribuíram direta ou indiretamente para o meu crescimento acadêmico pois, cada um de vocês tiveram um papel fundamental nesta jornada, e por isso, levo todos no coração como parte integrante desta conquista.

SUMÁRIO

RESUMO

Este trabalho de conclusão de curso tem como objetivo fornecer uma visão técnica sobre cibersegurança e seus mecanismos de proteção. O cenário atual revela uma crescente incidência de quebras de segurança em todo o mundo, causadas por ataques hackers cada vez mais sofisticados. O estudo começa relatando alguns casos recentes de violações de segurança, destacando suas consequências e impactos em diversos setores. Serão abordados exemplos de empresas, organizações governamentais e indivíduos afetados por esses ataques, demonstrando a importância da cibersegurança nos dias de hoje. Em seguida, serão explorados os diferentes tipos de ataques hackers utilizados atualmente, desde ataques por vírus, ransomware, até intrusões de rede e exploração de vulnerabilidades. Posteriormente, serão apresentados mecanismos e ferramentas de proteção contra esses ataques. Por fim, um estudo de caso será realizado em uma empresa com o objetivo de avaliar e propor soluções para mitigar e proteger-se contra esses ataques cibernéticos. Serão identificados os principais pontos vulneráveis da empresa, bem como as medidas de segurança necessárias para proteger seus ativos digitais, considerando as melhores práticas da indústria e conformidade com os padrões e regulamentos de segurança. Este trabalho busca contribuir para a compreensão dos desafios enfrentados atualmente em termos de segurança cibernética, fornecendo também um panorama das ameaças e mecanismos de proteção disponíveis. Espera-se que as informações e recomendações apresentadas neste estudo possam auxiliar organizações e indivíduos a fortalecerem suas defesas contra ataques hackers e preservarem a integridade de seus dados e sistemas.

Palavras chaves: segurança cibernética, cibersegurança, segurança em redes

Abstract

The current scenario reveals a growing incidence of security breaches worldwide, caused by increasingly sophisticated hacker attacks. The study begins by reporting some recent cases of security breaches, highlighting their consequences and impacts across various sectors. Examples of companies, government organizations, and individuals affected by these attacks will be addressed, demonstrating the importance of cybersecurity in today's world. Subsequently, the different types of hacker attacks currently used will be explored, ranging from virus attacks and ransomware to network intrusions and vulnerability exploitation. Later, protection mechanisms and tools against these attacks will be presented. Finally, a case study will be conducted in a company with the aim of assessing and proposing solutions to mitigate and protect against these cyber attacks. The main vulnerable points of the company will be identified, as well as the necessary security measures to protect its digital assets considering industry best practices and compliance with security standards and regulations. This work seeks to contribute to the understanding of the challenges currently faced in terms of cybersecurity, providing an overview of threats and available protection mechanisms. It is hoped that the information and recommendations presented in this study can assist organizations and individuals in strengthening their defenses against hacker attacks and preserving the integrity of their data and systems.

Keywords: cybersecurity, network security, cyber security.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

IBGE - Instituto Brasileiro de Geografia e Estatística
DDoS - *Distributed Denial of Service*
RPS - *Remote Procedure Call*
HTTP - *Hypertext Transfer Protocol*
IoT - *Internet of Things*
LAN - *Local Area Network*
MAN - *Metropolitan Area Network*
WAN - *Wide Area* Network
IEEE - *Institute of Electrical and Electronics Engineers*
OSI - *Open Systems Interconnection*
SQL - *Structured Query Language*
IA - Inteligência Artificial
PROX - *Proxy*
VPN - *Virtual Private Network*
IP - *Internet Protocol*
IDS - *Intrusion Detection System*
IPS - *Intrusion Prevention System*
LGPD - Lei Geral de Proteção de Dados (Brasil)
CIO - *Chief Information Officer*
CISO - *Chief Information Security Officer*
TI - Tecnologia da Informação

1 INTRODUÇÃO

1.1 CONTEXTO E JUSTIFICATIVA

A segurança cibernética tem se tornado uma preocupação cada vez mais relevante em escala global devido ao aumento da acessibilidade e ao crescente desenvolvimento da internet em todo o mundo. A era digital trouxe inúmeros benefícios e oportunidades, mas também trouxe desafios significativos relacionados à proteção das informações e aos riscos associados aos ataques cibernéticos.

Segundo dados do IBGE a internet está acessível a 90% dos domicílios brasileiros e esta expansão segue em diversos países, consequentemente, este avanço tecnológico e a interconexão de dispositivos têm exposto organizações a ameaças cibernéticas que podem causar prejuízos financeiros, danos à reputação, comprometimento da confidencialidade, integridade e disponibilidade dos dados. Esta crescente dependência de sistemas de informação e a ampliação do acesso à internet têm criado um cenário propício para a ocorrência de ataques cibernéticos a empresas, governos e indivíduos (IBGE, 2022).

A recente quebra de segurança em empresas de renome mundial tem chamado a atenção para a importância da segurança cibernética. Casos emblemáticos como o vazamento de dados do Facebook, e o ataque à Equifax, empresa de crédito norte-americana que sofreu danos irreparáveis, atingiram 143 milhões de seus consumidores nos Estados Unidos. Outro caso foi o ransomware WannaCry em 2017, que afetou mais de 230.000 PCs Windows em 150 países em apenas um dia, muitos deles em agências governamentais e hospitais demonstram o impacto significativo que tais incidentes podem ter na escala global. No âmbito brasileiro, ataques ao Tribunal Superior Eleitoral e outras instituições também ressaltam a vulnerabilidade das organizações nacionais diante dessas ameaças.

Em outubro de 2023, Google, Amazon e Cloudflare anunciaram a detecção e neutralização do maior ataque distribuído de negação de serviço (DDoS) da história. O ataque ocorreu em agosto e envolveu 7,5 vezes mais solicitações por segundo (RPS) do que o ciberataque recorde anterior, atingindo um pico de 398 milhões de RPS. Isso resultou em mais solicitações do que o total de visualizações de artigos da Wikipédia em um mês. O ataque explorou uma falha de segurança no protocolo

HTTP/2, conhecida como "Reinicialização rápida HTTP/2", uma falha de segurança de *dia zero*, que sobrecarregou os sites, tornando-os temporariamente indisponíveis. As empresas conseguiram mitigar o ataque, atualizando suas defesas à medida que aprendiam sobre a nova técnica dos invasores. O Google neutralizou os ataques na borda da rede enquanto a Amazon e a Cloudflare registraram picos de 155 milhões e 201 milhões de RPS, respectivamente. Os ataques DDoS representam uma ameaça significativa para as organizações, causando perda de tempo e recursos na recuperação (MOZELLI, 2023).

O aumento na acessibilidade à internet tem impulsionado o crescimento exponencial do uso de tecnologias digitais, tanto por indivíduos quanto por empresas e governos. A disseminação de dispositivos conectados, a expansão da Internet das Coisas (IoT) e a crescente digitalização de processos têm proporcionado benefícios significativos, mas também têm ampliado o espaço para ações maliciosas. A facilidade de comunicação e transmissão de dados em tempo real, aliada à complexidade das redes de informação, cria um ambiente propício para os ataques cibernéticos.

Diante desse contexto, é imprescindível adotar medidas eficientes de segurança para proteger os sistemas e os dados sensíveis das organizações. A implementação de mecanismos de prevenção, detecção e resposta a incidentes cibernéticos torna-se essencial para mitigar riscos e garantir a continuidade das operações.

Este trabalho tem como objetivo analisar os mecanismos de prevenção utilizados na segurança e sua eficácia na proteção. Serão abordados casos recentes de quebra de segurança em empresas brasileiras e mundiais, destacando as lições aprendidas e as consequências desses incidentes. A compreensão desses aspectos contribuirá para a identificação de melhores práticas e estratégias de segurança cibernética no contexto atual.

1.2 OBJETIVO

O propósito deste trabalho consiste em sistematizar os principais tipos de ataque, mecanismos de segurança e ferramentas relacionadas à segurança cibernética que podem ajudar em uma organização. Os objetivos específicos são os seguintes:

- Identificar os principais tipos de ataque (tanto humanos quanto tecnológicos) que comprometem a segurança da informação de uma empresa
- Relacionar os mecanismos de segurança aos tipos de ataque na atualidade.
- Realizar uma pesquisa sobre ferramentas computacionais que implementam os mecanismos de segurança mais eficientes.
- Selecionar uma organização para avaliar a viabilidade da implementação das ferramentas estudadas e verificar a eficácia da sistematização elaborada.

1.3 METODOLOGIA

Para realizar este trabalho, será conduzida uma pesquisa bibliográfica, que será composta principalmente por livros, artigos de periódicos e materiais disponíveis na internet. O objetivo é interpretar, compreender e analisar os dados e ações relevantes usando recursos e técnicas apropriados.

Na segunda etapa, será realizado um estudo dos principais problemas relacionados a ataques cibernéticos e segurança da informação que comprometem a infraestrutura de uma empresa.

A terceira etapa consiste em identificar os mecanismos e ferramentas de segurança que podem ser empregados contra os diferentes tipos de ataques emergentes.

A etapa quatro envolve a escolha de uma organização para implementar a estratégia operacional analisada e, posteriormente, validar e aprimorar as recomendações desenvolvidas na etapa três.

Por fim, a última etapa abrange a análise e avaliação dos resultados obtidos com o objetivo de sugerir melhorias nas recomendações relacionadas.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 TOPOLOGIA DE REDES

A estrutura fundamental de uma rede de telecomunicações consiste em um conjunto de módulos de processamento interconectados por meio de um sistema de comunicação, como demonstrado na figura 1. Esses módulos de processamento, comumente referidos como nós da rede, podem abranger estações de trabalho, servidores e outros dispositivos de rede.

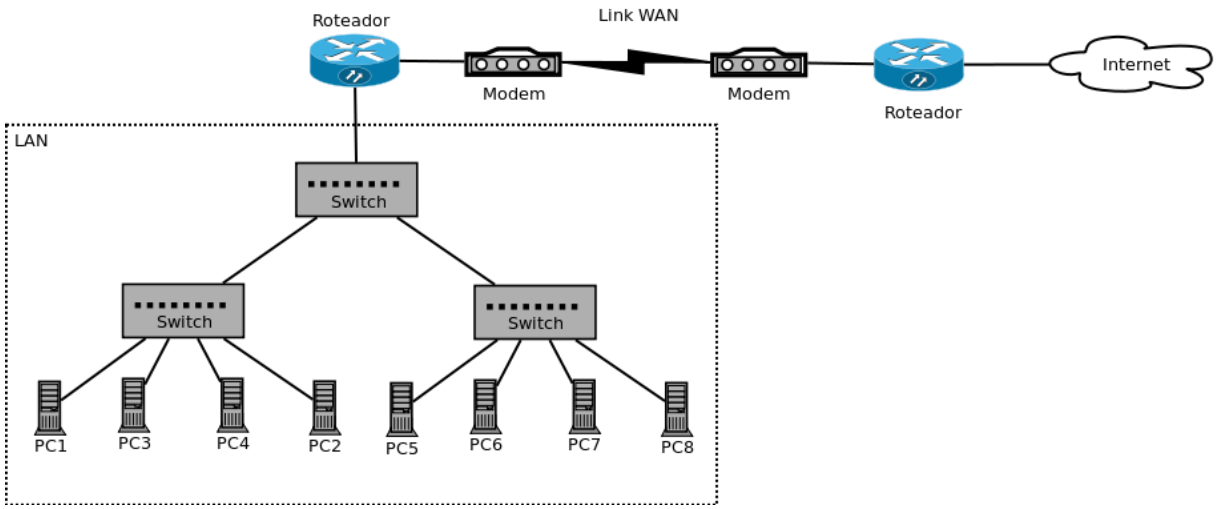

Figura 1: Rede de Telecomunicações

Fonte: https://wiki.sj.ifsc.edu.br/index.php/RCO20704-2014-1

O sistema de comunicação estabelece uma configuração topológica que interconecta os diversos módulos processadores por meio de conexões físicas, juntamente com um conjunto de regras e convenções para organizar a comunicação, conhecido como protocolos. Em termos simples, a topologia representa o padrão de organização da rede de computadores.

A escolha da topologia a ser empregada é uma decisão crucial na criação de um sistema de comunicação. Naturalmente, as opções disponíveis dependem do tipo de rede (LAN, MAN ou WAN), pois determinadas topologias são mais apropriadas para cada tipo de rede. Além disso, a topologia de uma rede desempenha um papel significativo em relação à eficiência, flexibilidade e segurança.(SOARES *et al.* 1995)

As conexões físicas em uma topologia podem ser classificadas em dois tipos: ponto a ponto e multiponto. Na conexão física ponto a ponto, dois módulos processadores (ou nós) estão interligados através de um meio de transmissão que permite a transferência direta de dados, conforme ilustrado na figura 2.

Figura 2: Topologia ponto a ponto
Fonte: autoria própria

Na topologia multiponto, ocorre a interligação de três ou mais módulos processadores (ou nós), possibilitando o compartilhamento do mesmo meio de transmissão, conforme exemplificado na figura 3. As várias configurações topológicas são criadas com base em combinações desses dois tipos de conexões físicas: ponto a ponto e multiponto.

Figura 3: Topologia multiponto
Fonte: autoria própria

2.2 CAMADAS DE REDES

No modelo de referência OSI, a estrutura é composta por sete camadas, cada uma com funções específicas na comunicação de dados, formando uma hierarquia que facilita a comunicação entre sistemas. Cada nível fornece serviços bem definidos para o nível superior, criando uma estrutura organizada para a transmissão de dados. (TANENBAUM, 2003)

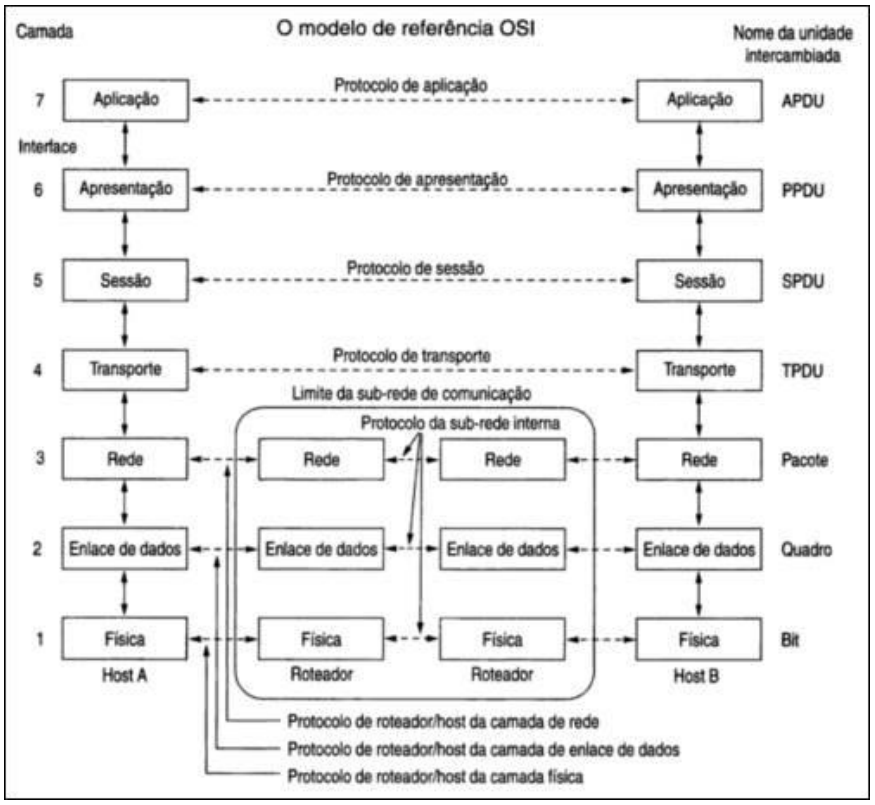

Figura 4: Modelo de Referência OSI
Fonte: TANENBAUM, 2003

Camada Física: responsável pela transmissão de bits brutos, lidando com interfaces mecânicas, elétricas e de sincronização, gerenciando o meio físico de transmissão abaixo da camada de enlace.

Camada de Enlace de Dados: realiza a divisão da informação em quadros ou pacotes, transmitindo-os sequencialmente, permitindo ao receptor enviar confirmações de maneira eficiente.

Camada de Rede: controla e supera problemas de lentidão causados por múltiplos pacotes sendo transmitidos simultaneamente, lidando com o roteamento dos dados.

Camada de Transporte: recebe a informação da camada acima, certificando-se da sua divisão, se necessário, garantindo a entrega correta e concluindo o envio eficientemente.

Camada de Sessão: controla quem envia e recebe dados, evitando o envio simultâneo de operações críticas, permitindo a retomada do envio de dados após interrupções na navegação.

Camada de Apresentação: facilita a comunicação entre computadores com diferentes representações de dados, gerenciando o intercâmbio abstrato de dados juntamente com o código padrão durante a conexão.

Camada de Aplicação: localiza-se no topo da pilha e contém vários protocolos necessários para os usuários, englobando as interfaces utilizadas pelos aplicativos para se comunicarem sobre a rede

2.3 PRINCIPAIS PROTOCOLOS DE REDE

Segundo TANENBAUM (2011) os protocolos consistem em conjuntos de regras desenvolvidos para facilitar a comunicação entre as diferentes camadas do modelo OSI. Essas normas desempenham o controle tanto do formato quanto do significado das informações transmitidas. Para KUROSE e ROSS os protocolos definem o formato e a ordem das mensagens enviadas e recebidas pelas entidades da rede bem como as ações que são tomadas quando da transmissão ou recepção de mensagens. Aqui é possível destacar os principais protocolos:

TCP/IP (Transmission Control Protocol/Internet Protocol): Um conjunto de protocolos amplamente usado para comunicação na Internet e redes locais. O TCP garante a entrega confiável de dados, enquanto o IP endereça e roteia os pacotes.

DNS (Domain Name System): Um protocolo que traduz nomes de domínio em endereços IP, permitindo que os usuários acessem recursos online usando nomes amigáveis.

HTTP/HTTPS (Hypertext Transfer Protocol/Secure): Protocolos utilizados para transferir páginas da web e outros recursos online. O HTTPS acrescenta segurança por meio de criptografia.

Protocolos de envio e recebimento de mensagens: O SMTP (Simple Mail Transfer Protocol) é usado para enviar mensagens, enquanto o POP (Post Office Protocol) e o IMAP (Internet Message Access Protocol) são usados para receber e armazenar emails. Além disso, o protocolo TLS/SSL é frequentemente aplicado para criptografar comunicações de email, garantindo segurança.

SSH: Secure Shell (SSH), cuja tradução livre para o português seria algo como "Cofre Seguro", é um protocolo de rede desenvolvido para reforçar a segurança na troca de arquivos entre os sistemas computacionais envolvidos, ou seja, o cliente e o servidor. O SSH opera por meio de um processo de login e senha, permitindo verificar e autenticar a legitimidade do servidor que o cliente pretende acessar, proporcionando uma conexão mais segura entre ambas as partes.

FTP: Protocolo de Transferência de Arquivos (FTP) é um dos pioneiros na rede, proporcionando uma maneira simples, rápida e versátil de transferir arquivos entre dois computadores pela internet. Funciona com dois tipos de conexão: a do cliente, que solicita a conexão, e a do servidor, que aceita o pedido e fornece os dados requisitados. Já o Protocolo de Transferência Simples de Arquivos, ou SFTP, opera de forma semelhante ao FTP, adicionando uma camada adicional de segurança. A autenticação da conexão entre os computadores (cliente e servidor) oferece mais proteção aos arquivos transferidos. O usuário pode personalizar a quantidade de arquivos transmitidos simultaneamente e estabelecer senhas para reforçar a segurança, graças à tecnologia SSH.

2.4 PRINCIPAIS COMPONENTES DE REDES

Switches

Um switch de rede (também chamado de hub de comutação, hub de ponteamento e, pela IEEE, ponte MAC) é um hardware de rede que conecta dispositivos em uma rede de computadores usando comutação de pacotes para receber e encaminhar dados para o dispositivo de destino. A comutação de pacotes

permite que os dados sejam enviados pela rede de telecomunicações em rajadas curtas ou "pacotes" que contêm números de sequência para que possam ser reconstituídos no destino.

Um switch de rede é uma ponte de rede de vários portos que utiliza endereços MAC para encaminhar dados na camada de link de dados (camada 2) do modelo OSI. Alguns switches também podem encaminhar dados na camada de rede (camada 3) ao incorporar funcionalidades de roteamento. Tais switches são comumente conhecidos como switches de camada 3 ou switches de camadas múltiplas.

Os switches são blocos de construção essenciais para qualquer rede, eles conectam vários dispositivos como computadores, pontos de acesso sem fio, impressoras e servidores na mesma rede dentro de um prédio ou campus. Um switch permite que os dispositivos conectados compartilhem informações e se comuniquem entre si.

Roteadores

Enquanto os switches permitem a comunicação entre diferentes dispositivos em uma rede, os roteadores possibilitam a comunicação entre diferentes redes.

Um roteador é um dispositivo que conecta duas ou mais redes ou sub-redes de comutação de pacotes. Ele desempenha duas funções principais: gerenciar o tráfego entre essas redes encaminhando pacotes de dados para seus endereços IP pretendidos, e permitir que vários dispositivos usem a mesma conexão à Internet. Existem vários tipos de roteadores, mas a maioria deles encaminha dados entre LANs (redes locais) e WANs (redes de longa distância).

Uma LAN é um grupo de dispositivos conectados restrito a uma área geográfica específica e geralmente requer um único roteador. Uma WAN, por outro lado, é uma grande rede espalhada por uma vasta área geográfica. Grandes organizações e empresas que operam em várias localidades em todo o país, por exemplo, precisarão de LANs separadas para cada local, que se conectam às outras LANs para formar uma WAN. Como uma WAN é distribuída por uma grande área, muitas vezes requer vários roteadores e switches.

Gateway

Enquanto um roteador é utilizado para unir dois tipos semelhantes de redes, um gateway é utilizado para unir duas redes dissimilares. O termo "dissimilar" pode ser usado para descrever redes que utilizam diferentes protocolos principais. Um gateway é um dispositivo de hardware que atua como uma "porta" entre duas redes. Pode ser um servidor, firewall, roteador ou outro dispositivo que possibilita o fluxo de tráfego por toda a rede. Gateways funcionam como ponto de entrada e saída para uma rede, pois todos os dados devem passar por um gateway de comunicação antes de serem roteados. Na maioria das redes baseadas em IP, o único tráfego que não passa por pelo menos um gateway é o tráfego entre nós no mesmo segmento de rede local (LAN).

Firewalls

Um Firewall é um dispositivo de segurança de rede que monitora e filtra (aceita, rejeita ou descarta) o tráfego de rede de entrada e saída com base nas políticas de segurança previamente estabelecidas por uma organização. Em sua forma mais básica, um firewall é essencialmente a barreira que fica entre uma rede interna privada e a Internet pública. O principal propósito de um firewall é permitir a passagem de tráfego inofensivo e impedir a entrada de tráfego perigoso. (ROJANALA, 2022)

2.5 AMEAÇAS E VULNERABILIDADES EM REDES

À medida que as redes se tornam mais interconectadas e essenciais para as operações cotidianas, é fundamental compreender as várias maneiras pelas quais essas redes podem ser exploradas por atacantes mal-intencionados. Essa compreensão é essencial para implementar estratégias eficazes de segurança cibernética e proteger a integridade e a confidencialidade das informações transmitidas.

2.5.1 Principais Ameaças

As redes de telecomunicações estão sujeitas a uma ampla gama de ameaças cibernéticas que podem causar danos significativos, algumas das ameaças comuns incluem:

2.5.1.1 Vírus

Os vírus são programas com a capacidade de modificar dados ou sistemas, destruir arquivos, alterar programas ou executar funções inesperadas em sistemas computacionais ou dispositivos informatizados (JESUS, 2016). Inicialmente, esses códigos maliciosos eram disseminados por programadores que buscavam exibir suas habilidades, sem causar danos às vítimas, visando tornar-se celebridades no mundo hacker. No entanto, atualmente, os vírus são frequentemente utilizados por atividades criminosas com o intuito de roubar dados ou prejudicar sistemas de outros usuários.

É importante destacar que os vírus não têm a capacidade de se autoexecutar; é necessário que o usuário os execute para iniciar a contaminação. Portanto, se um vírus estiver presente em um HD, CD ou pen drive, ele não terá efeito algum até que seja deliberadamente executado por alguém. Contrariamente a um mito popular, os vírus não têm o poder de danificar o hardware do equipamento, uma vez que são softwares e não podem queimar ou quebrar dispositivos físicos.(CASSANTI, 2014).

2.5.1.2 Worm

Denominado como verme, esse tipo de código malicioso caracteriza-se por residir na memória ativa do computador e se reproduzir automaticamente, dispensando qualquer ação por parte do usuário. Ele comumente se instala em computadores e programas que apresentam vulnerabilidades, sendo a desatualização uma das principais. Os Worms consomem consideráveis recursos do computador, resultando na degradação do desempenho e, potencialmente, no preenchimento do disco rígido devido à multiplicação constante de cópias de si mesmos (WENDT; JORGE, 2013).

2.5.1.3 Cavalo de troia

O Cavalo de Troia é um arquivo aparentemente inofensivo entregue por meio de diversos disfarces, como um cartão digital, um álbum de fotos, um protetor de tela ou jogos, por exemplo. O componente principal executa suas funções normais, enquanto o componente malicioso opera de maneira oculta ao usuário (CASSANTI, 2014).

Uma vez que o sistema é infectado, o invasor pode adquirir controle administrativo da máquina, permitindo a alteração de configurações de segurança e tornando o computador mais vulnerável. Além disso, há a possibilidade de capturar informações do usuário e enviá-las por e-mail ao criminoso (JESUS, 2016).

2.5.1.4 Botnets

Botnets referem-se a redes de computadores compostas por vários bots, que são sistemas instalados por criminosos em estações de servidores e que respondem a comandos e funções enviados a eles. Os computadores afetados tornam-se "zumbis", e devido ao grande número de máquinas invadidas, a identificação da origem torna-se desafiadora (JESUS, 2016).

Uma das principais finalidades das Botnets é facilitar ataques de Negativa Distribuída de Serviço (DDoS), nos quais diversos computadores enviam solicitações a um servidor específico, sobrecarregando-o e tornando o serviço inacessível. Em termos de investigação, as autoridades policiais geralmente começam identificando um computador usado no ataque e, em seguida, aplicam a engenharia reversa por meio da análise dos códigos maliciosos. Esse processo permite descobrir para onde as informações estão indo ou de onde estão vindo (WENDT; JORGE, 2013).

2.5.1.5 Spywares

Os spywares são programas espiões projetados para coletar informações sobre o usuário, seus padrões de acesso e preferências. Essas informações são enviadas pela Internet, geralmente para fins publicitários ou para a coleta de dados pessoais. Embora compartilhem semelhanças com os cookies de sites, que armazenam preferências do usuário, como idioma, fonte e cor, os spywares

diferenciam-se por utilizar essas ações de maneira maliciosa. Sua propagação assemelha-se à dos cavalos de Troia, embora sua finalidade não seja manipular ou dominar o sistema do usuário por parte de invasores (CASSANTI, 2014).

2.5.1.6 Rootkits

O termo rootkit deriva da combinação das palavras "root", que se refere ao usuário de computador que possui controle total sobre o sistema nas plataformas Unix, e "kit", que designa programas utilizados por usuários do sistema operacional Linux para obter controle total sobre um sistema comprometido. Esses programas permanecem ocultos no computador e podem ser instalados localmente por alguém com acesso ao sistema ou remotamente, por meio de outro computador (CASSANTI, 2014).

Devido à sua capacidade de ocultar chaves no registro e processos no gerenciador de tarefas, a maioria dos antivírus enfrenta dificuldades para detectar rootkits. No ambiente Windows, esses arquivos maliciosos podem gerar mensagens de erro, frequentemente indicando a inexistência de arquivos ao tentar abrir determinados programas. Além disso, há o risco de que esses arquivos contenham outros malwares infiltrados, como keyloggers e vírus (WENDT; JORGE, 2013).

2.5.1.7 Backdoor

Um backdoor é uma ferramenta de administração remota que possibilita o controle de um computador por meio de uma rede ou da internet. Ele consiste em um cliente, que é o atacante, e um servidor, que é a máquina alvo. Esse tipo de software oferece diversas funcionalidades, incluindo a capacidade de criar, excluir e executar comandos, modificar configurações do sistema e registros do Windows, ajustar configurações de desligamento, capturar informações de login, registrar teclas pressionadas, capturar a tela do computador e até mesmo ativar a webcam para monitorar o ambiente na residência da vítima (CASSANTI, 2014).

2.5.1.8 Phishing

O termo "phishing" tem sua origem no verbo inglês "to fish", que significa pescar, e descreve a prática de pescar informações de usuários. Inicialmente, o termo era usado para descrever a fraude de envio de e-mails não solicitados, nos quais a vítima era induzida a acessar sites fraudulentos. Uma característica marcante desse tipo de ataque é a criação de mensagens que aparentam ser originárias de fontes legítimas, como bancos, órgãos governamentais ou empresas. Atualmente, a palavra também é empregada para descrever a ação de pessoas que enviam mensagens com o objetivo de persuadir vítimas a fornecer informações pessoais aos criminosos (WENDT; JORGE, 2013).

2.5.1.9 DoS

O ataque de Negação de Serviço, ou Denial of Service (DoS), é caracterizado por sobrecarregar um serviço informático até que ele se torne inacessível. Esses ataques podem adotar várias formas, como o método de inundação de pacotes, que envolve o envio de uma grande quantidade de pacotes de rede para congestionar o link, impedindo o acesso de usuários legítimos. O ataque por problemas de protocolo explora deficiências nos protocolos utilizados para a comunicação com os clientes.

Outra abordagem é o ataque por problemas de codificação, que explora vulnerabilidades no software, como o Buffer Overflow, no qual dados são inseridos no software além dos limites de memória configurados, geralmente resultante de falhas de desenvolvimento sem verificações adequadas. O ataque de disco visa preencher o disco de informações até torná-lo inoperante.

Um método significativo é o ataque de Distributed Denial of Service (DDoS), amplamente utilizado atualmente. Esse tipo de ataque envolve a utilização de várias máquinas para realizar ataques simultâneos de inundação de pacotes. A vantagem desse método é que o tráfego gerado por várias máquinas é muito mais volumoso do que o de uma única máquina, aumentando a eficácia do ataque (JESUS, 2016).

2.5.1.10 Quebra de senha

Existem três tipos reconhecidos de ataques visando a quebra de senhas. Um deles é o método de força bruta, que consiste em tentar todas as combinações possíveis, muitas vezes utilizando ferramentas automatizadas. Outro método é o ataque de dicionário, que testa palavras comumente encontradas em dicionários. O terceiro método é conhecido como "rainbow table", utilizado para quebrar senhas criptografadas. Nesse método, os hashes das senhas são comparados com uma tabela predefinida de hashes já calculados, facilitando a identificação da senha correspondente (JESUS, 2016).

2.5.1.11 SQL injection

Essa técnica envolve a modificação de parâmetros ou instruções executadas em uma ou mais tabelas de um banco de dados por meio da linguagem Structured Query Language (SQL). Essa prática possibilita o acesso não autorizado, a alteração ou a destruição de informações no banco de dados (JESUS, 2016).

2.5.1.12 Sniffer

Essa técnica tem o objetivo de monitorar todo o tráfego de rede TCP/IP, possibilitando a interceptação e análise de todos os dados transmitidos. Se um usuário estiver navegando em sites sem criptografia (HTTP), todas as informações, incluindo senhas de acesso, podem ser visualizadas. A captura desse tráfego é realizada por programas conhecidos como sniffers, os quais podem ser empregados tanto por empresas para monitorar as atividades de seus funcionários quanto por criminosos interessados em obter informações como logins, senhas, sites acessados e conteúdos sigilosos trocados por e-mail (WENDT; JORGE, 2013).

2.5.1.13 Ransomware

O ransomware é considerado um dos malwares mais temidos pelos usuários devido à forma como impactam suas vítimas. Em suas primeiras manifestações, esse tipo de malware bloqueia a tela do computador, exibindo uma mensagem que

exigia pagamento para liberar o sistema. Com o sucesso inicial, surgiram diversas variantes mais perigosas. As novas versões têm a capacidade de criptografar os arquivos do dispositivo, exibindo informações sobre como proceder para obter a chave de desbloqueio. O pagamento costuma ser solicitado em Bitcoins, uma moeda eletrônica independente de qualquer autoridade central. Vale ressaltar que efetuar o pagamento não garante o desbloqueio dos arquivos, pois a identificação do criminoso é difícil, e não há garantia de responsabilização(TREND MICRO, 2015).

2.5.2 Vulnerabilidades em Redes de Telecomunicações

As redes de telecomunicações possuem várias vulnerabilidades que podem ser exploradas pelos atacantes. Essas vulnerabilidades podem incluir:

2.5.2.1 Tecnologias desatualizadas

Infraestrutura antiquada ou desatualizada pode resultar em sistemas pouco confiáveis e não seguros. A gestão deve reconhecer que, quando a tecnologia se torna obsoleta, há um risco de perda de integridade de dados devido a ataques. O planejamento estratégico da gestão deve sempre incluir uma análise da tecnologia atualmente em uso. Idealmente, um planejamento adequado por parte da gestão deve evitar que a tecnologia se torne obsoleta, mas quando a obsolescência se manifesta, a gestão deve tomar ações imediatas. Profissionais de TI desempenham um papel significativo na identificação da possível obsolescência.

Grandes quantidades de código de computador são escritas, depuradas, publicadas e vendidas antes que todos os seus bugs sejam detectados e resolvidos. Às vezes, combinações de determinado software e hardware revelam novos bugs e essas falhas variam de bugs a condições de falha não testadas. Às vezes, esses bugs não são erros, mas sim atalhos propositais deixados por programadores por razões benignas ou malignas. Coletivamente, rotas de acesso abreviadas para programas que contornam verificações de segurança são chamadas de "trap doors" e podem causar sérias violações de segurança.

Bugs de software são tão comuns que existem sites inteiros dedicados a documentá-los. Um dos mais frequentemente utilizados é o *Bugtraq*, que fornece

informações atualizadas sobre as últimas vulnerabilidades de segurança, bem como um arquivo muito abrangente de bugs passados.(WHITMAN; MATTORD, 2016)

2.5.2.2 Configurações Inseguras

Configurações inseguras em sistemas de redes telecomunicações representam uma ameaça significativa à segurança cibernética, pois introduzem vulnerabilidades que podem ser exploradas por atacantes. Um aspecto crítico relacionado às configurações inseguras é a presença de portas abertas inadequadamente. As portas, que funcionam como canais de comunicação, quando configuradas de maneira inadequada, podem fornecer pontos de entrada para invasores, permitindo acesso não autorizado a serviços e dados sensíveis. Contudo, a ausência de firewalls ou a configuração inadequada dessas barreiras de segurança pode resultar em impactos significativos para as organizações. Os firewalls desempenham um papel crucial na prevenção de tráfego não autorizado, e quando configurados de maneira inadequada, colocam em risco a integridade da rede. Os impactos decorrentes dessas falhas na segurança podem ser gigantescos, considerando as potenciais consequências de acessos não autorizados e comprometimento da infraestrutura de rede.

Outro ponto de vulnerabilidade está nas senhas, sendo senhas fracas uma forma comum de configuração insegura. Escolher senhas fáceis de adivinhar ou não atualizá-las regularmente aumenta o risco de acesso não autorizado. Além disso, o uso de padrões de autenticação predefinidos, como senhas de fábrica ou logins padrão, cria uma lacuna de segurança que os atacantes podem explorar facilmente.

A falta de criptografia adequada também torna-se uma preocupação, especialmente em ambientes nos quais os dados são transmitidos pela internet. Configurações inseguras muitas vezes resultam em falta de proteção durante a transmissão, expondo informações sensíveis a terceiros mal-intencionados. (WHITMAN;MATTORD, 2016).

2.5.2.3 Falta de conscientização e erros humanos

Esta categoria inclui ações realizadas sem intenção ou propósito malicioso por um usuário autorizado. Quando as pessoas usam sistemas de informação, erros acontecem. A inexperiência, treinamento inadequado e suposições incorretas são apenas algumas coisas que podem causar certos inconvenientes. Independentemente da causa, até mesmo erros inofensivos podem causar danos extensos. Por exemplo, o uso de um simples pendrive infectado por aplicações maliciosas.

Uma das maiores ameaças à segurança da informação de uma organização são os próprios colaboradores. Os colaboradores são os agentes de ameaça mais próximos dos dados organizacionais porque eles usam próprios dados para atividades cotidianas e conduzir os negócios da organização, contudo seus erros representam uma séria ameaça à confidencialidade, integridade, e disponibilidade desses dados, refletindo numa estreita relação com as ameaças externas. Isso ocorre porque os erros dos colaboradores podem facilmente levar a entrada de dados incorretos, exclusão acidental, modificação indevida, armazenamento em áreas não protegidas e até mesmo execuções de aplicações maliciosas.

Deixar informações classificadas críticas em áreas não protegidas, por exemplo, em um site da Web ou até mesmo na lixeira de uma estação de trabalho, pode custar caro à segurança da organização. Isto resulta em possíveis rastros para os invasores explorarem. Esses descuidos podem criar vulnerabilidades e assim gerar oportunidades para os atacantes. No entanto, se alguém danificar ou destruir dados de propósito, o ato pertence a uma categoria de ameaça diferente.(WHITMAN;MATTORD, 2016)

Ao compreender essas ameaças e vulnerabilidades, os profissionais de segurança cibernética podem implementar medidas proativas para mitigar os riscos e proteger as redes de telecomunicações contra ataques.

2.6 TÉCNICAS DE SEGURANÇA EM REDES DE TELECOMUNICAÇÕES

Nesta seção, exploraremos a importância de implementar técnicas avançadas de segurança em redes de telecomunicações para se proteger contra ameaças cibernéticas cada vez mais sofisticadas. A crescente complexidade dos ataques exige que as organizações adotem abordagens proativas e ferramentas atualizadas para garantir a integridade, confidencialidade e disponibilidade de suas redes e dados.

2.6.1 Importância das Técnicas de Segurança Avançadas

As ameaças cibernéticas evolui constantemente, com atacantes criando métodos mais sofisticados para explorar as vulnerabilidades e técnicas de segurança avançadas são essenciais por várias razões.

Um dos métodos usados pelos atacantes atualmente é a vulnerabilidade de dia zero, onde falhas são exploradas antes que os desenvolvedores tenham conhecimento. Logo, a equipe de desenvolvimento só fica ciente da vulnerabilidade após um possível ataque, e a partir desse momento, tem um "dia zero" para criar uma correção impedindo que o ataque seja bem-sucedido e possa se multiplicar.

Quando o hacker descobre a vulnerabilidade, ele começa a trabalhar em um *exploit*, desencadeando uma corrida contra o tempo na exploração da vulnerabilidade antes que os desenvolvedores possam descobrir.

Em resumo, um ataque de dia zero é uma violação de segurança que visa uma vulnerabilidade, geralmente com o uso de malware específico para esse fim. Após um ataque, os desenvolvedores devem se esforçar para identificar o incidente e compreender sua natureza, consequentemente criar um patch de atualização para correção.(FREDA,2021)

A Inteligência Artificial (IA) tem se destacado como uma tecnologia verdadeiramente revolucionária na detecção de anomalias em diversos setores, e a área de Tecnologia da Informação não é uma exceção. Uma das aplicações particularmente promissoras da IA reside na detecção de anomalias de rede, uma

vez que identificar ameaças e comportamentos suspeitos de forma precoce é de extrema importância para a segurança e a performance das redes corporativas. Adicionalmente, a IA também desempenha um papel crucial no combate ao ransomware, uma das ameaças que mais afetam as organizações mundialmente.

Detectar anomalias de rede é uma tarefa intrinsecamente desafiadora, dado que requer a habilidade de identificar comportamentos atípicos e suspeitos em meio a uma imensa quantidade de dados de tráfego de rede. É neste contexto que a Inteligência Artificial tem vindo a ser cada vez mais empregada para analisar padrões de tráfego de rede e identificar anomalias que possam sugerir atividades maliciosas ou problemas de desempenho.

A utilização de algoritmos de IA, como o aprendizado de máquina e redes neurais, permite às organizações construir modelos preditivos capazes de identificar comportamentos anômalos com uma precisão notável. Esses modelos podem ser treinados com base em dados históricos de tráfego de rede, o que lhes permite aprender a distinguir entre padrões normais e anormais. À medida que mais dados são processados e o sistema de IA é alimentado com informações atualizadas, sua capacidade de detecção de anomalias continua a aprimorar-se de modo constante. Isso representa um avanço significativo na segurança das redes e na proteção contra ameaças cibernéticas cada vez mais sofisticadas. (International IT,2023)

2.6.2 Utilização de Ferramentas Adequadas e Atualizadas

A eficácia das técnicas de segurança cibernética é fundamental para garantir a integridade e a disponibilidade das redes de telecomunicações. A utilização de ferramentas adequadas e constantemente atualizadas desempenha um papel vital nesse cenário dinâmico:

Firewalls Avançados: Firewalls de próxima geração são projetados para inspecionar o tráfego de forma mais profunda, identificando ameaças sofisticadas e aplicando políticas de segurança mais granulares.

Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS): IDS monitoram atividades suspeitas, enquanto os IPS têm a capacidade de bloquear

automaticamente ataques, essas ferramentas são essenciais para detectar e responder a intrusões em tempo real.

Sistemas de backups: Desempenham um papel crucial na garantia da disponibilidade e da integridade dos dados e das comunicações em um ambiente de telecomunicações. Esses sistemas são projetados para proteger informações críticas, minimizar o tempo de inatividade e garantir a continuidade dos serviços em caso de falhas ou desastres.

Gerenciamento de Identidade e Acesso: Sistemas de gerenciamento de identidade garantem que apenas usuários autorizados tenham acesso a recursos e ambientes específicos, minimizando o risco de acesso não autorizado.

Soluções de Aprendizado de Máquina: Ferramentas de aprendizado de máquina podem analisar grandes volumes de dados para identificar padrões e anomalias, detectando ameaças que podem passar despercebidas por abordagens tradicionais.

Ao adotar e integrar essas ferramentas avançadas e modernas, as organizações podem enfrentar os desafios de segurança cibernética de maneira mais eficaz, permanecendo à frente das ameaças em constante evolução. A combinação estratégica de técnicas avançadas e ferramentas atualizadas é fundamental para garantir uma proteção abrangente das redes de telecomunicações e dos dados confidenciais que transitam por elas.

2.7 ANÁLISE DE TÉCNICAS DE SEGURANÇA

2.7.1 Firewalls e Sistemas de Detecção de Intrusões (IDS/IPS)

Nesta seção será estudado o conceito de firewalls e seu Sistemas de Detecção de Intrusões (IDS/IPS), ambos são componentes fundamentais na proteção de redes de telecomunicações contra ameaças cibernéticas. Vamos analisar a importância de cada uma delas, seus propósitos e suas funcionalidades.

2.7.1.1 Conceito Firewalls

Os firewalls são um dos elementos essenciais para proteger redes de telecomunicações. Eles atuam como uma barreira entre uma rede interna e a Internet ou outra rede externa. O principal objetivo de um firewall é controlar o tráfego de rede com base em regras de segurança predefinidas, ele decide quais pacotes de dados são permitidos ou bloqueados com base em políticas de segurança.

Os firewalls podem operar em vários níveis, incluindo firewalls de camada de aplicação (proxy), firewalls de inspeção de estado (stateful) e firewalls de camada de pacotes. Alguns firewalls também oferecem funcionalidades de VPN (Rede Virtual Privada) para criptografar a comunicação.

As regras de acesso são configuradas pelos administradores para determinar como o tráfego é tratado, e isso inclui a especificação de portas, protocolos e endereços IP permitidos ou bloqueados. Os firewalls desempenham um papel crucial na prevenção de ataques, como ataques DDoS e intrusões externas ajudando na garantia que apenas o tráfego autorizado seja permitido na rede interna.(NORTHCUTT, Stephen; NOVAK, Judy.2002)

2.7.1.2 Sistemas de Detecção de Intrusões (IDS) e Sistemas de Prevenção de Intrusões (IPS)

Os IDS e IPS são tecnologias complementares que monitoram o tráfego de rede em busca de atividades suspeitas. Eles são fundamentais para detectar e responder a ameaças em tempo real.

Os Sistemas de Detecção de Intrusões (IDS) monitoram o tráfego em busca de padrões ou comportamentos anômalos que possam indicar uma possível intrusão, gerando alertas quando detectam atividades suspeitas.

Os Sistemas de Prevenção de Intrusões (IPS) não apenas detectam ameaças, mas também podem tomar ação para bloqueá-las automaticamente. Eles aplicam políticas de segurança para bloquear ou limitar o tráfego suspeito.

Os IDS e IPS usam assinaturas, análise comportamental e heurística para identificar ameaças, podem também monitorar tráfego de rede, logs e atividades de usuário.

A combinação de firewalls, IDS e IPS é uma abordagem eficaz para a segurança cibernética em redes de telecomunicações. Os firewalls controlam o acesso, enquanto os IDS e IPS detectam e respondem a ameaças em tempo real, garantindo que a rede permaneça protegida contra uma ampla gama de ameaças cibernéticas.(NORTHCUTT, Stephen; NOVAK, Judy.2002)

2.7.2 Sistema de Antivírus

Os sistemas antivírus são componentes críticos na defesa contra ameaças cibernéticas, principalmente malware, que inclui vírus, worms, trojans e outros tipos de software malicioso. Nesta explicação técnica, vamos explorar como os sistemas antivírus funcionam, seus principais componentes e os métodos utilizados para identificar e neutralizar ameaças.

2.7.2.1 Funcionamento baśico de um antivírus

Os antivírus utilizam várias técnicas para garantir a segurança de um sistema. Isso inclui a coleta de dados sobre arquivos e programas no sistema, como tamanhos, datas de criação e conteúdo binário. A principal abordagem é a verificação de assinaturas de vírus, que são padrões binários exclusivos associados a ameaças já conhecidas e mantidas em um banco de dados pelo antivírus.

Quando um arquivo é acessado ou executado, o antivírus verifica seu conteúdo em busca de assinaturas de vírus, se houver uma correspondência, o antivírus identifica e neutraliza a ameaça. Em caso de identificação de um arquivo

como malicioso, o antivírus pode movê-lo para quarentena, isolando-o para que não cause danos. O usuário geralmente tem a opção de remover ou restaurar o arquivo proporcionando controle sobre a gestão de ameaças detectadas. Essas medidas são essenciais para conter efetivamente qualquer ameaça e garantir a segurança do sistema.

2.7.2.2 Técnicas Avançadas de Análise

Embora a verificação de assinaturas seja eficaz contra ameaças conhecidas, muitos sistemas antivírus adotam abordagens mais avançadas para detectar ameaças desconhecidas. Atualmente, os antivírus utilizam algoritmos heurísticos que identificam comportamentos suspeitos, como a tentativa de modificar registros do sistema ou a comunicação com servidores remotos.

Esses métodos vão além da simples correspondência de assinaturas e incluem análise comportamental. Alguns antivírus monitoram ativamente o comportamento de programas em execução, identificando atividades maliciosas, como tentativas de autoreplicação. Além disso, o uso de técnicas de sandboxing é comum, permitindo que antivírus executem arquivos suspeitos em ambientes isolados, conhecidos como "sandboxes", para observar seu comportamento sem afetar o sistema principal. Essas abordagens mais avançadas fortalecem a capacidade dos antivírus de detectar e neutralizar ameaças desconhecidas, contribuindo para uma segurança mais robusta do sistema.

2.7.2.3 Atualização de Definições

A eficácia de um antivírus depende da atualização constante de suas definições de vírus. Novas ameaças são descobertas regularmente, e as definições precisam ser atualizadas para identificá-las. Os fabricantes de antivírus fornecem atualizações periódicas que incluem novas assinaturas de vírus e melhorias nas técnicas de detecção.

2.7.2.4 Integração com o Sistema Operacional

Os antivírus são geralmente integrados ao sistema operacional, eles interceptam solicitações de arquivos e ações do sistema para verificar a presença de

ameaças antes de permitir o acesso. Isso é conhecido como "proteção em tempo real."

2.7.2.5 Limitações e Evolução

Embora os sistemas antivírus sejam uma parte vital da segurança cibernética, eles têm limitações. Pois a evolução das ameaças merece atenção, como o malware polimórfico que muda de forma dificultando a detecção por assinaturas. Portanto, a segurança cibernética moderna incorpora sistemas de prevenção de intrusões, análise de comportamento e soluções de segurança em várias camadas para fornecer uma proteção abrangente.

2.7.3 Controle de Acesso

O controle de acesso assegura a integridade e confidencialidade, abrangendo a administração dos indivíduos autorizados a acessar recursos ou áreas específicas em uma rede de telecomunicações, sob condições específicas. Esse processo é executado por meio da autenticação e da autorização.

2.7.3.1 Autenticação

É o processo de verificar a identidade de um usuário ou dispositivo, isso geralmente envolve a combinação de algo que o usuário sabe (como uma senha) com algo que o usuário possui (como um token de segurança) ou algo que é inerente à identidade do usuário (como uma impressão digital).

2.7.3.2 Autorização

Após a autenticação bem-sucedida, a autorização determina quais recursos ou áreas o usuário ou dispositivo pode acessar e quais operações podem ser realizadas, esta situação é controlada por meio de políticas de segurança.

2.7.4 Política de Segurança

A prevenção de acesso não autorizado, a proteção de dados sensíveis, a conformidade legal e a resposta a incidentes são práticas fundamentais para garantir a segurança cibernética em redes de telecomunicações. Essas políticas de segurança são essenciais para evitar o acesso não autorizado a informações sensíveis, proteger dados confidenciais contra exposição ou roubo, e garantir a conformidade com regulamentos como a Lei Geral de Proteção de Dados (LGPD).

A implementação efetiva de controle de acesso e políticas de segurança desempenha um papel crucial na gestão de riscos de segurança cibernética. Além de contribuir para a proteção contra ameaças internas e externas, essas práticas garantem que apenas usuários autorizados tenham acesso a recursos e dados sensíveis. Além disso, a clareza e eficácia dessas políticas facilitam a identificação e resposta rápida a incidentes de segurança, fortalecendo ainda mais a postura de segurança da rede de telecomunicações.

2.7.4.1 Diretrizes de políticas de segurança

As políticas de segurança são diretrizes e regras que definem como a segurança deve ser mantida em uma rede de telecomunicações. Elas incluem:

Políticas de Acesso: Estabelecem quem tem permissão para acessar quais recursos. Por exemplo, uma política pode determinar que apenas funcionários autorizados têm acesso à rede interna.

Políticas de Senhas: Definem os requisitos de senha, como complexidade e rotação regular. Senhas fortes são essenciais para prevenir acesso não autorizado.

Políticas de Monitoramento: Estabelecem procedimentos para monitorar atividades de rede em busca de comportamento suspeito. Isso pode incluir a revisão de logs e alertas de segurança.

Políticas de Backup e Recuperação: Definem como os dados devem ser regularmente copiados e armazenados em locais seguros para recuperação em caso de falha ou ataque.

2.7.5 Sistema de Backups

Um sistema de backup desempenha um papel fundamental em qualquer ambiente de tecnologia da informação e sua importância é indispensável e pode ser analisada sob diversos aspectos:

2.7.5.1 Redundância e Resiliência

Um sistema de backup oferece redundância aos dados e sistemas críticos de uma rede de telecomunicações. Isso significa que, em caso de falha, seja ela de hardware, software, erro humano, desastre natural ou ciberataque, os dados e serviços podem ser rapidamente restaurados a partir do backup, minimizando interrupções e mantendo a continuidade das operações.

2.7.5.2 Proteção contra Perda de Dados

As redes de telecomunicações lidam com grandes volumes de dados, incluindo informações críticas de clientes e configurações de rede. A perda de dados pode ser devastadora, resultando em prejuízos financeiros, danos à reputação e até mesmo questões legais. Um sistema de backup eficaz ajuda a proteger contra a perda irreparável de informações valiosas.

2.7.5.3 Recuperação Rápida

A capacidade de recuperar rapidamente após uma falha é essencial em redes de telecomunicações, onde a disponibilidade constante é crucial. Com backups adequados, é possível minimizar o tempo de inatividade e os impactos negativos nas operações.

2.7.5.4 Conformidade com Regulamentações

Em muitos setores, incluindo telecomunicações, existem regulamentações estritas relacionadas à retenção de dados e à recuperação em caso de desastres. Ter um sistema de backup adequado ajuda a atender a esses requisitos e evitar penalidades legais.

2.7.5.5 Prevenção de Ameaças Cibernéticas

Os ciberataques estão se tornando cada vez mais sofisticados, e os sistemas de telecomunicações estão entre os alvos mais visados. Ransomware e outros tipos de malware podem bloquear o acesso aos dados, mas um sistema de backup off-site (fora das instalações) pode ser a única maneira de recuperar os dados sem ceder às demandas dos criminosos.

2.7.5.6 Evolução e Atualização

À medida que as redes de telecomunicações evoluem e são atualizadas, é importante garantir que as configurações antigas e os dados históricos possam ser recuperados quando necessário. Um sistema de backup bem planejado ajuda a garantir que informações críticas não sejam perdidas durante transições de tecnologia.

2.7.5.7 Recuperação de Desastres

Eventos imprevisíveis, como incêndios, terremotos e inundações, podem causar danos severos às infraestruturas de telecomunicações. Um sistema de backup que inclui cópias de dados e sistemas em locais geograficamente dispersos ajuda na recuperação após desastres, permitindo a continuidade das operações.

Em resumo, um sistema de backup é uma parte crítica da estratégia de gerenciamento de riscos e continuidade de negócios em redes de telecomunicações. Ele oferece proteção contra uma variedade de ameaças e ajuda a garantir a confiabilidade e a disponibilidade dos serviços de telecomunicações, o que é essencial para atender às necessidades dos clientes e manter a competitividade no mercado. Portanto, sua implementação e manutenção adequadas são investimentos essenciais para qualquer operadora de telecomunicações.

3 DESAFIOS DE SEGURANÇA EM REDES DE TELECOMUNICAÇÕES

De acordo com a pesquisa "Enterprise Networks in Transition: Taming the Chaos", a segurança representa o principal desafio na gestão de redes, e esses desafios se intensificam à medida que as arquiteturas das redes corporativas se tornam mais complexas.

Simultaneamente, o aumento do volume de ameaças cibernéticas e a diversidade de aplicações adotadas pelos usuários corporativos também apresentam novos desafios para a administração eficiente dos recursos de rede.

Para lidar com esse cenário desafiador, organizações, quando possível, devem incorporar ferramentas que permitam monitorar proativamente seu ambiente de TI. Além disso, contar com especialistas dedicados que trabalhem continuamente para ajustar as configurações de acordo com as necessidades de desempenho e segurança das redes é fundamental.

No entanto, muitas empresas enfrentam limitações financeiras para investir em recursos destinados à gestão de redes, fortalecimento da segurança e obtenção de maior visibilidade.

3.1 AMEAÇAS CIBERNÉTICAS EMERGENTES

As ameaças cibernéticas emergentes representam um desafio constante para indivíduos, empresas e organizações em todo o mundo. À medida que a tecnologia evolui, novas formas de ataques cibernéticos surgem. Aqui estão algumas das ameaças cibernéticas emergentes mais significativas a serem consideradas:

Ataques de Ransomware Avançados: Ransomware não é uma ameaça nova, mas os ataques de ransomware estão se tornando mais sofisticados e direcionados, onde os cibercriminosos agora adotam táticas como a exfiltração de dados[1] antes de criptografá-los, o que aumenta a pressão sobre as vítimas para pagar resgates.

[1] A exfiltração de dados ocorre quando uma pessoa autorizada extrai dados dos sistemas protegidos a que eles pertencem e os compartilha com terceiros não autorizados ou transfere esses dados para sistemas inseguros. fonte: https://www.psafe.com/blog/o-que-e-a-exfiltracao-de-dados/

Deepfake e Manipulação de Mídia: A tecnologia de deepfake permite a criação de vídeos e áudios falsos altamente convincentes, que podem ser usados para difamar pessoas, manipular informações e criar cenários de desinformação. Isso representa uma ameaça significativa para a integridade das informações e a reputação das pessoas e organizações.

Ataques à Infraestrutura Crítica: Ciberataques direcionados a infraestruturas críticas, como redes elétricas, sistemas de água e transporte, são uma ameaça emergente preocupante. Esses ataques podem causar interrupções significativas e ter impactos reais na segurança pública.

Ataques a Dispositivos IoT (Internet das Coisas): À medida que mais dispositivos são conectados à internet, a superfície de ataque aumenta. Os dispositivos IoT geralmente têm medidas de segurança insuficientes e podem ser alvos de ataques para espionagem, controle remoto ou inclusão em botnets.

Ataques de Engenharia Social Aprimorados: Os ataques de engenharia social continuam sendo uma ameaça significativa, mas estão se tornando mais direcionados e personalizados. Os cibercriminosos usam informações obtidas nas redes sociais e outras fontes para criar ataques mais convincentes.

Exploração de Vulnerabilidades de Zero-Day: A exploração de vulnerabilidades de zero-day, que são falhas de segurança desconhecidas pelos desenvolvedores e não corrigidas, continua sendo uma ameaça. Os atores maliciosos podem usá-las para ganhar acesso não autorizado a sistemas e redes.

Ataques à Cadeia de Suprimentos: Os atacantes agora visam fornecedores e parceiros de negócios como uma maneira de atingir organizações maiores. Comprometendo um fornecedor, os criminosos podem ganhar acesso a sistemas e dados de suas metas reais.

Ataques em Nuvem: Com o aumento da adoção de serviços em nuvem, os atacantes estão direcionando suas atividades para essas plataformas. Eles buscam explorar configurações incorretas, fraquezas de segurança e credenciais comprometidas para acessar recursos em nuvem.

Criptomoedas e Ataques de Mineração Maliciosa: Os cibercriminosos estão cada vez mais envolvidos em atividades de mineração de criptomoedas

maliciosas, infectando computadores e redes para gerar moedas digitais sem o consentimento dos proprietários.

Ataques Quânticos (potencial): Embora ainda estejamos nos estágios iniciais, o desenvolvimento da computação quântica tem o potencial de quebrar muitos dos algoritmos criptográficos atuais, exigindo a adoção de novas abordagens de segurança cibernética.

Para proteger-se contra essas ameaças cibernéticas emergentes, é crucial manter sistemas, aplicativos e dispositivos atualizados, adotar práticas de segurança cibernética sólidas, educar os funcionários sobre ameaças de engenharia social e investir em soluções de segurança avançadas, como detecção de ameaças baseada em inteligência artificial e machine learning. Além disso, a colaboração com outras organizações e compartilhamento de informações sobre ameaças também são essenciais para manter-se à frente dos cibercriminosos.

3.2 GERENCIAMENTO DE INCIDENTES DE SEGURANÇA

De acordo com Feres e Lopes (2021), a gestão de incidentes em Segurança da Informação engloba uma série de processos, como detecção, alerta, avaliação, resposta, tratamento e aprendizado. Atualmente, essa gestão tornou-se de extrema importância especialmente diante da crescente transição do mundo físico para o digital. Logo, a necessidade de uma proteção legislativa mais robusta também se intensificou, sendo contemplada pelo Marco Civil da Internet, Lei n° 12.965/2014, e pela Lei Geral de Proteção de Dados, Lei nº 13.709/2018. Além disso, o aumento significativo no número de ataques cibernéticos destaca ainda mais a relevância dessas medidas de segurança.

O objetivo final do gerenciamento de incidentes é minimizar o impacto e as consequências, bem como melhorar a postura da segurança nas organizações. Aqui estão os principais aspectos do gerenciamento de incidentes de segurança:

Preparação: A preparação é a fase inicial do gerenciamento de incidentes, isso envolve a criação de políticas, procedimentos e diretrizes de segurança, bem como a definição de papéis e responsabilidades da equipe de resposta aos incidentes. Além disso, é importante estabelecer uma estrutura de comunicação para informar as partes interessadas internas e externas sobre incidentes.

Detecção e Relatórios: A detecção precoce de incidentes é crucial. Isso pode ser alcançado por meio de sistemas de monitoramento de segurança, detecção de intrusões, análise de logs e outras ferramentas de segurança. Quando um incidente é detectado, ele deve ser relatado imediatamente à equipe de resposta a incidentes.

Classificação e Avaliação: Após a detecção, os incidentes são classificados com base em sua gravidade e impacto potencial. A avaliação determina o escopo do incidente, quais sistemas ou recursos foram afetados e qual a probabilidade de comprometimento de dados ou interrupção dos serviços.

Resposta: A resposta a incidentes envolve ação imediata para conter, neutralizar e resolver o incidente. Isso pode incluir isolar sistemas comprometidos, remover malware, corrigir vulnerabilidades e restaurar serviços afetados. A equipe de resposta a incidentes deve seguir os procedimentos predefinidos e tomar medidas para minimizar o impacto do incidente.

Comunicação: Comunicar eficazmente durante um incidente é fundamental. Isso inclui informar as partes interessadas internas e externas, como a alta administração, reguladores, clientes e a opinião pública, dependendo da natureza do incidente. A comunicação transparente e precisa ajuda a construir confiança e minimiza danos à reputação.

Investigação e Análise: Após a resolução inicial do incidente, uma investigação mais aprofundada é realizada para entender as causas, a extensão do dano e as táticas utilizadas pelos invasores. Isso ajuda a identificar pontos fracos na segurança que precisam ser abordados para evitar incidentes futuros.

Recuperação: Depois de conter e resolver o incidente, a organização concentra-se na recuperação. Isso envolve a restauração de sistemas e serviços afetados, a revisão das políticas de segurança e a implementação de melhorias para evitar incidentes semelhantes no futuro.

Documentação e Lições Aprendidas: É importante documentar todas as ações tomadas durante o gerenciamento do incidente. Isso inclui relatórios, registros de atividades e análises pós-incidentes. A organização deve aprender com cada incidente para fortalecer sua postura de segurança.

Melhoria Contínua: O gerenciamento de incidentes de segurança não é um processo único. É um ciclo contínuo de melhoria. Com base nas lições aprendidas, a organização deve aprimorar constantemente suas políticas, procedimentos e medidas de segurança.

Conformidade Regulatória: Em muitos setores, as regulamentações exigem que as organizações tenham processos de gerenciamento de incidentes de segurança em vigor. Cumprir essas regulamentações é fundamental para evitar penalidades legais.

Em resumo, o gerenciamento de incidentes de segurança é uma parte essencial da estratégia de segurança cibernética de uma organização. Ele permite que a organização identifique, responda e se recupere de incidentes de segurança de maneira eficaz, protegendo seus ativos e minimizando os impactos negativos. Uma abordagem proativa e bem planejada para o gerenciamento de incidentes é fundamental em um cenário de ameaças cibernéticas em constante evolução.

3.3 ASPECTOS LEGAIS E REGULATÓRIOS

Os aspectos legais e regulatórios desempenham um papel fundamental na governança da segurança cibernética e na proteção de dados de uma organização.

Com o aumento das ameaças cibernéticas e a crescente conscientização sobre a importância da privacidade, várias leis e regulamentações foram promulgadas em todo o mundo para definir padrões mínimos de segurança cibernética e proteção de dados. Aqui estão alguns dos principais aspectos legais e regulatórios relacionados à segurança cibernética e à proteção de dados:

Regulamentações de Proteção de Dados: Em várias jurisdições, como a União Europeia com o Regulamento Geral de Proteção de Dados (GDPR), os Estados Unidos com a Lei de Privacidade do Consumidor da Califórnia (CCPA), no Brasil a Lei Geral de Proteção de Dados (LGPD) entre outras, existem regulamentações estritas que estabelecem direitos e obrigações para organizações em relação à coleta, armazenamento, processamento e compartilhamento de dados pessoais. Essas regulamentações exigem medidas específicas de segurança

cibernética, notificação de violações e conformidade com padrões rigorosos de privacidade.

Leis de Notificação de Violação: Muitas jurisdições exigem que as organizações notifiquem as autoridades regulatórias e os indivíduos afetados quando ocorre uma violação de dados pessoais. As notificações devem ser feitas dentro de prazos específicos e podem ter implicações legais significativas se não forem cumpridas.

Leis Setoriais: Em setores específicos, como serviços financeiros e saúde, existem regulamentações adicionais que impõem requisitos específicos de segurança cibernética. Por exemplo, a Lei de Responsabilidade e Portabilidade do Seguro de Saúde (HIPAA) nos Estados Unidos exige medidas rigorosas de segurança para proteger informações de saúde.

Ciberseguro: Muitas organizações estão adquirindo apólices de ciberseguro para ajudar a mitigar os riscos financeiros associados a violações de segurança cibernética. A conformidade com as regulamentações de segurança cibernética pode ser um fator importante na determinação do custo e da elegibilidade para o ciberseguro.

Padrões de Segurança: Além de regulamentações específicas, existem padrões de segurança reconhecidos internacionalmente, como o ISO 27001 juntamente com a ISO 27002, que estabelece diretrizes para o gerenciamento de segurança da informação. O cumprimento desses padrões pode ser uma evidência valiosa de que uma organização está tomando medidas adequadas para proteger seus ativos de informações.

Responsabilidade Legal: As organizações podem ser responsabilizadas legalmente por falhas na segurança cibernética que resultem em danos a terceiros. Isso pode incluir ações judiciais de indivíduos afetados, reguladores e parceiros de negócios.

Requisitos de Auditoria e Relatórios: Algumas regulamentações exigem que as organizações passem por auditorias de segurança cibernética e relatem regularmente seu estado de conformidade. Isso pode ser necessário para manter licenças ou certificações específicas.

Responsabilidade dos Executivos: Em alguns casos, os executivos de alto nível, como o diretor de tecnologia (CIO) e o diretor de segurança da informação (CISO), podem ser responsabilizados legalmente por violações de segurança cibernética se não tomarem medidas adequadas para proteger a organização.

Cooperação Internacional: Muitos incidentes cibernéticos envolvem atores que operam em jurisdições estrangeiras. A cooperação internacional é cada vez mais importante para investigar e combater ameaças cibernéticas.

Em resumo, o cenário legal e regulatório em relação à segurança cibernética e à proteção de dados está em constante evolução e é altamente complexo. As organizações devem estar cientes das leis e regulamentos aplicáveis em sua jurisdição e setor, adotar práticas de segurança cibernética robustas para cumprir essas regulamentações e estar preparadas para responder a incidentes de segurança cibernética de acordo com as exigências legais e regulatórias específicas. O não cumprimento dessas regulamentações pode resultar em penalidades significativas e danos à reputação. Portanto, a conformidade legal é uma parte crítica da estratégia de segurança cibernética de uma organização.

4. ESTUDO DE CASO

4.1 DEFINIÇÃO SOBRE O ESTUDO DE CASO

Neste estudo de caso, exploraremos um incidente ocorrido na empresa LabX, uma organização que atua na área de médica, no qual um ataque cibernético afetou severamente suas operações. Este incidente em questão resultou na paralisação do serviço em um período de 12 horas. O ataque foi desencadeado por um vírus ransomware que se espalhou pela rede, criptografando arquivos essenciais do servidor. Suspeita-se que o ataque possa ter tido origem em um usuário com permissões de administrador, com acesso às pastas do servidor. Importante notar que a máquina desse usuário, que ocupava uma posição de gerência, estava executando o sistema operacional Windows 7 e usava um antivírus nativo que estava desatualizado na época do incidente, que ocorreu em 2021.

Diante da urgência da situação, a equipe de TI da LabX tomou medidas imediatas para conter o incidente, sendo uma das primeiras ações a desconexão física dos cabos de rede tanto dos computadores do usuário suspeito quanto do servidor afetado. Além disso, foi necessário adotar uma solução drástica para restaurar a funcionalidade do sistema, que envolveu a formatação das máquinas afetadas e posteriormente a restauração do backup e reinstalação dos softwares afetados.

Este estudo de caso tem como objetivo analisar em detalhes o incidente de segurança cibernética ocorrido na LabX, incluindo as causas prováveis do ataque, as medidas de resposta imediatas tomadas pela equipe de TI e as lições aprendidas com o incidente. Ao compreender as circunstâncias que levaram a esse incidente e as ações subsequentes, a LabX busca melhorar sua postura de segurança cibernética e estar mais preparada para lidar com ameaças emergentes no futuro.

Levantamento de Ativos

Este cenário atual da organização deve nortear a base para o estudo de caso em segurança cibernética. O conhecimento e a identificação dos ativos são fundamentais para avaliar riscos e implementar medidas de segurança adequadas e garantir a continuidade operacional.

Os ativos de TI identificados incluem:

Servidores Ubuntu:

- Servidor de Produção: Neste servidor fica instalado o ERP(Sistema Integrado de Gestão Empresarial), sistema de software integrado que permite a uma organização gerenciar e automatizar uma variedade de processos de negócios essenciais, como atendimento ao cliente, finanças, contabilidade, recursos humanos, compras, gestão de estoque e produção.
- Servidor Shadow: Este servidor tem o papel de duplicar ou espelhar os serviços e dados do servidor principal(produção), de modo que, se o servidor principal sofrer uma falha, o servidor shadow possa entrar em operação rapidamente, minimizando a interrupção dos serviços.

Servidor de Automação (Windows 10):

- Este servidor é dedicado a tarefas de automação e é uma parte vital da infraestrutura.

Servidor Windows Server 2016 com Máquinas Virtuais (VMs):

- O servidor Windows Server 2016 abriga duas máquinas virtuais (VMs) que desempenham funções importantes na organização. Uma VM é dedicada a serviços de comunicação interna, como chats, enquanto a outra atua como um repositório de arquivos central e backups automáticos . Essas VMs suportam a colaboração e o compartilhamento de arquivos, essenciais para as rotinas dos setores administrativos.

Desktops:

- A organização possui um total de 101 desktops, disponíveis para as atividades diárias dos colaboradores. Dentre esses desktops, 32 ainda operam com o sistema operacional Windows 7, enquanto os demais foram atualizados para o Windows 10.

Esse levantamento abrange tanto os ativos de hardware quanto os sistemas operacionais utilizados. É importante observar que a diversidade de sistemas operacionais (Ubuntu, Windows 10, Windows Server 2016, Windows 7) introduz desafios específicos em termos de gerenciamento e segurança cibernética. A avaliação e a proteção adequada desses ativos são de importância crítica para garantir a segurança da infraestrutura de TI da organização.

4.2 METODOLOGIA DE IMPLANTAÇÃO E AVALIAÇÃO

A segurança cibernética é uma preocupação fundamental para empresas que buscam proteger seus ativos de informações e garantir a continuidade de suas operações em um ambiente cada vez mais hostil em termos de ameaças digitais. Neste contexto, foi sugerido à empresa LabX um plano para mitigar esses tipos de ataques e assim reconhecendo a importância de fortalecer suas defesas contra ataques cibernéticos, foi realizada uma pesquisa abrangente para identificar e implementar novas ferramentas que ajudassem a mitigar essas ameaças.

4.2.1. INSTALAÇÃO DE UM FIREWALL DE ÚLTIMA GERAÇÃO (PFSENSE)

Um dos pilares centrais da estratégia de segurança cibernética sugerido à empresa foi a implementação de um firewall de última geração. Após avaliar diversas opções, a empresa escolheu o pfSense como sua solução de firewall.

O pfSense é uma plataforma de firewall de código aberto que oferece um alto grau de flexibilidade e personalização, isso permite à empresa adaptar-se às necessidades específicas de segurança, definindo regras de filtragem de tráfego personalizadas e implementar políticas de segurança robustas.

O firewall ainda oferece recursos avançados, como filtragem de conteúdo, balanceamento de carga, VPN(Virtual Private Network), IDS/IPS (detecção/prevenção de intrusão) e muito mais. Essas capacidades avançadas ajudam a proteger a rede da empresa contra uma variedade de ameaças cibernéticas.

Como uma solução de código aberto (Open Source), o pfSense oferece uma alternativa altamente custo-efetiva em comparação com outras soluções comerciais de firewall, isto sem comprometer a segurança e o desempenho.

4.2.2. INSTALAÇÃO DE UM ANTIVÍRUS COM GERENCIAMENTO EM NUVEM (KASPERSKY)

Além do firewall, a empresa reconheceu a importância de estabelecer uma defesa sólida e completa contra malwares, vírus e outras ameaças cibernéticas. Portanto, foi aconselhado implementar a solução antivírus Kaspersky com gerenciamento em nuvem, uma escolha baseada em diversas razões que demonstram sua eficácia e confiabilidade.

O Kaspersky é amplamente reconhecido como um dos principais fornecedores de soluções de segurança cibernética no mercado, tem sólida reputação, é respaldada por anos de experiência e tem uma base de clientes em todo o mundo que confia em sua capacidade de fornecer proteção eficaz.

O Kaspersky oferece uma defesa completa contra uma variedade de ameaças cibernéticas, incluindo vírus, malware, Trojans, ransomware e muito mais. Sua abordagem de proteção em várias camadas é projetada para evitar que essas ameaças prejudiquem seus dispositivos e dados. Com recursos de antivírus em tempo real, o Kaspersky monitora constantemente os dispositivos e sistemas, identificando e neutralizando qualquer ameaça em potencial.

A solução também protege contra downloads nocivos e sites falsos que tentam capturar dados pessoais, isto garante uma navegação segura na internet, prevenindo a exposição a sites maliciosos e ataques de phishing que buscam informações sensíveis.

Além disso, o antivírus oferece um recurso de detecção de stalkerware[2], que alerta se algum aplicativo nos dispositivos da empresa pode ser usado para espionar e rastrear as atividades dos usuários. Essa funcionalidade protege a privacidade dos

[2] Um stalkerware é um tipo de vírus (malware) desenvolvido para “perseguir” ou monitorar a vítima. https://www.hardware.com.br/artigos/o-que-e-stalkerware/

funcionários e ajuda a manter um ambiente seguro e livre de vigilância não autorizada.

A implementação do Kaspersky com gerenciamento em nuvem não apenas fornece uma camada adicional de segurança cibernética, mas também simplifica a administração e o monitoramento da segurança em toda a organização. A equipe de TI da empresa poderá acompanhar e responder a incidentes de maneira eficiente, garantindo a proteção contínua dos ativos contra ameaças cibernéticas em constante evolução.

4.2.3. INSTALAÇÃO DE UM WINDOWS SERVER E CONFIGURAÇÃO DO ACTIVE DIRECTORY PARA CONTROLE DE USUÁRIO

Para reforçar o controle de acesso e a gestão de usuários, a empresa optou por implementar um servidor Windows e configurar o Active Directory. Essa medida estratégica oferece várias vantagens:

Controle de Acesso: O Active Directory permite à empresa controlar quem tem acesso a quais recursos de rede, pastas compartilhadas e aplicativos. Isso ajuda a evitar acessos não autorizados e reforça a segurança.

Gerenciamento de Políticas: Através do Active Directory, a empresa pode definir políticas de segurança, políticas de senha e outras diretrizes que melhoram a postura geral de segurança.

Centralização de Contas de Usuário: A centralização das contas de usuário simplifica a gestão de credenciais e facilita a adição e remoção de usuários, melhorando a eficiência operacional.

4.2.4. INSTALAÇÃO DE UM SISTEMA DE BACKUP (OWNCLOUD)

O ownCloud é uma plataforma de software livre de gerenciamento de dados e compartilhamento de arquivos que oferece recursos de backup como parte de suas funcionalidades gerais. Embora não seja um sistema de backup dedicado, o ownCloud pode ser configurado para fornecer benefícios de backup para organizações e usuários que desejam proteger seus dados. Alguns dos benefícios do uso do ownCloud como parte de um sistema de backup incluem:

Armazenamento e compartilhamento de arquivos: O ownCloud permite armazenar arquivos em um servidor centralizado, facilitando o acesso e compartilhamento de documentos, imagens e outros tipos de arquivos. Isso ajuda a proteger seus dados, pois eles são centralizados em um local seguro.

Sincronização de dados: O ownCloud oferece recursos de sincronização que permitem manter cópias locais dos seus arquivos em dispositivos pessoais, como computadores e dispositivos móveis. Isso ajuda a garantir que os dados estejam disponíveis mesmo se o servidor principal falhar.

Controle de versões: O ownCloud mantém um histórico de versões de arquivos, o que é útil para recuperar versões anteriores em caso de erros ou modificações indesejadas.

Segurança: O ownCloud possui recursos avançados de segurança, incluindo a capacidade de criptografar os dados armazenados e em trânsito, protegendo assim seus arquivos de acesso não autorizado.

Redundância de dados: Pode-se configurar o ownCloud para armazenar dados em vários locais, fornecendo redundância e maior proteção contra falhas.

Recuperação de desastres: Se o servidor principal do ownCloud falhar devido a um desastre, como um problema de hardware ou uma falha no sistema, você ainda poderá acessar seus dados em outros dispositivos ou locais de armazenamento.

Integração com sistemas de backup: Você pode integrar o ownCloud com sistemas de backup tradicionais para criar uma solução de backup mais completa podendo incluir a programação de backups regulares para garantir a proteção contínua dos dados.

Colaboração eficiente: O ownCloud permite a colaboração em tempo real em documentos e arquivos, facilitando o trabalho em equipe. Isso ajuda a garantir que as versões mais recentes dos documentos sejam sempre acessíveis e protegidas.

Acessibilidade em qualquer lugar: O ownCloud é acessível de qualquer lugar com conexão à internet, permitindo que você acesse seus arquivos e dados de

qualquer dispositivo, facilitando a recuperação de dados em caso de perda ou corrupção.

Controle de permissões: O ownCloud oferece recursos avançados de controle de permissões, permitindo que os administradores de sistema definam quem pode acessar, modificar ou excluir arquivos. Isso ajuda a proteger os dados contra exclusões acidentais ou intencionais.

4.2.5. ATUALIZAÇÃO DOS SISTEMAS OPERACIONAIS WINDOWS 7 PARA WINDOWS 10

Atualizar os sistemas operacionais da empresa para versões mais recentes, como a migração do Windows 7 para o Windows 10, é uma decisão crucial para manter a segurança e eficiência da infraestrutura de TI. Aqui estão alguns argumentos para destacar a importância dessa atualização:

Correções de Segurança: A Microsoft e outras empresas de software lançam atualizações de segurança regularmente para corrigir vulnerabilidades e ameaças conhecidas. O Windows 7 não está mais recebendo atualizações de segurança, tornando os sistemas que o utilizam vulneráveis a novos ataques cibernéticos. Atualizar para o Windows 10 garante que sua empresa continue recebendo atualizações críticas de segurança.

Conformidade com Regulamentações: Muitas regulamentações governamentais e setoriais exigem que as organizações mantenham seus sistemas operacionais atualizados para proteger dados sensíveis e informações do cliente. A não conformidade pode resultar em penalidades financeiras e perda de confiança dos clientes.

Proteção contra Ameaças Emergentes: As ameaças cibernéticas estão sempre evoluindo. Sistemas operacionais mais antigos têm mais probabilidade de serem alvos de ataques, pois os cibercriminosos procuram vulnerabilidades não corrigidas. O Windows 10 oferece melhorias de segurança, como o Windows Defender, que ajuda a proteger contra ameaças emergentes.

Desempenho e Eficiência: Versões mais recentes dos sistemas operacionais tendem a ser mais eficientes e oferecer melhor desempenho. Isso

resulta em uma produtividade aprimorada, menor tempo de inatividade e economia de custos a longo prazo.

Compatibilidade de Software: À medida que os desenvolvedores de software lançam novas versões de aplicativos, eles geralmente se concentram na compatibilidade com os sistemas operacionais mais recentes. Usar um sistema operacional desatualizado pode levar a problemas de compatibilidade e limitações no uso de software essencial para seus negócios.

Melhorias de Produtividade: O Windows 10 oferece uma variedade de recursos e melhorias que podem aumentar a produtividade da equipe, como a interface amigável, maior integração com serviços em nuvem e recursos de colaboração aprimorados.

Investimento a Longo Prazo: Atualizar para o Windows 10 é um investimento no futuro da sua empresa. Manter sistemas operacionais desatualizados pode resultar em custos imprevistos devido a falhas de segurança, perda de dados e interrupções nos negócios.

Reputação da Empresa: Manter sistemas atualizados mostra aos clientes, parceiros e partes interessadas que você leva a segurança de dados a sério. Isso contribui para uma melhor reputação da empresa e confiança do público.

4.2.6. CRIAÇÃO DE POLÍTICAS DE SEGURANÇA BASEADAS NA LGPD (LEI GERAL DE PROTEÇÃO DE DADOS)

A empresa, estando comprometida com a proteção da privacidade e dos dados pessoais de seus clientes e funcionários, adotou uma política de segurança que está alinhada com a Lei Geral de Proteção de Dados (LGPD). A LGPD é uma regulamentação brasileira que estabelece regras claras para o tratamento de dados pessoais e impõe obrigações específicas às organizações que lidam com esses dados. Abaixo, destacamos aspectos importantes dessa política:

Coleta e Tratamento Responsável de Dados: A política de segurança da empresa estabelece diretrizes para a coleta responsável de dados pessoais, garantindo que apenas as informações necessárias sejam coletadas e tratadas de acordo com as finalidades legais.

Consentimento e Transparência: A política enfatiza a importância do consentimento informado ao coletar dados pessoais e promove a transparência no tratamento de dados, fornecendo informações claras sobre como os dados são usados.

Medidas de Segurança: A política define medidas de segurança cibernética que visam proteger os dados pessoais contra vazamentos, perdas e acessos não autorizados. Isso inclui a implementação de controles técnicos, como criptografia, e práticas de segurança sólidas.

Direitos dos Titulares de Dados: A política reconhece e respeita os direitos dos titulares de dados, incluindo o direito de acesso, correção, exclusão e portabilidade de seus dados pessoais. A empresa X está preparada para atender a essas solicitações de acordo com a LGPD.

Treinamento e Conscientização: A empresa investe em treinamento e conscientização de seus funcionários para garantir que todos compreendam a importância da LGPD e estejam cientes de suas responsabilidades na proteção de dados pessoais.
https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/guia-orientativo-aplicacao-da-lgpd.pdf

4.2.7. INSTALAÇÃO DE UM SOFTWARE PARA GERENCIAMENTO DE INCIDENTES

A gestão de incidentes em Tecnologia da Informação é uma questão crítica, especialmente devido à elevada dependência tecnológica na atualidade. É crucial reconhecer que interrupções podem resultar em prejuízos comerciais e perda de dados.

Dessa maneira, as organizações devem estar aptas a lidar com essas situações, contando com um planejamento de contingência bem elaborado. Isso possibilita minimizar de maneira eficaz os impactos negativos desses eventos.

Registro: Ao receber um alerta sobre um incidente, o primeiro passo consiste em registrá-lo para iniciar o processo de correção. Embora simples, essa etapa é

fundamental para assegurar que a operação siga o protocolo estabelecido. Além disso, esse procedimento possibilita:

- Criar um histórico dos eventos relacionados a cada usuário.
- Obter estatísticas sobre a frequência de ocorrência de determinada situação.
- Identificar áreas nas quais concentrar esforços para melhorias nos sistemas e serviços.
- Garantir uma salvaguarda legal em caso de desfecho adverso.
- Alimentar o fluxo que conduz à resolução da problemática.

Identificação: Se a meta do gerenciamento de incidentes em TI é resolver a situação rapidamente, acelerar a identificação do problema é crucial. Para isso, práticas como questionar, compreender, alinhar expectativas e aplicar a escuta ativa são essenciais.

É fundamental assegurar uma comunicação efetiva com a parte afetada. Utilizar um roteiro de perguntas pode ajudar o atendente a otimizar esse processo, garantindo que nenhuma informação seja omitida.

Categorização: Compreendendo o incidente, a categorização é necessária para garantir que receba a atenção adequada. Priorizar urgências e encaminhar para o nível de suporte apropriado dependem dessa etapa. Portanto, é crucial estabelecer critérios para classificação e tags que identifiquem as condições, facilitando busca e compreensão rápidas. Manter o status sempre atualizado é vital para um monitoramento eficaz.

Investigação: A gestão de incidentes em TI requer que o atendente ou especialista encarregado da resolução compreenda completamente o cenário, desde suas causas até a situação atual. Isso é essencial para investigar soluções potenciais e avaliar os riscos associados a cada opção.

Nesse momento, uma base de consulta com informações sobre como agir em diferentes cenários, correlacionando as origens dos problemas com as ações corretivas e seus possíveis efeitos negativos, é uma ferramenta indispensável.

Resolução: Após analisar as opções e escolher um plano de ação, concentra-se na fase de resolução do problema. Além de propor ou aplicar soluções, essa etapa envolve testar as opções, estabelecendo um processo iterativo de feedback para alcançar o resultado desejado.

Fechamento: Cada etapa anterior deve ser registrada para formar um histórico das decisões tomadas e detalhes sobre como o incidente foi resolvido. O fechamento consiste em adicionar dados faltantes e verificar a precisão das informações. É um momento de avaliação, possibilitando a identificação de oportunidades de melhoria no protocolo.

4.3 RESULTADOS ESPERADOS

Com a implementação das ferramentas e dos métodos de segurança cibernética propostos é possível antecipar alguns resultados, tais como:

Aprimoramento da Segurança da Rede: A instalação de um firewall de última geração (pfSense) deve resultar em um aumento significativo na segurança da rede. Espera-se que o firewall ajude a proteger a rede contra ameaças externas, filtrando o tráfego indesejado e detectando possíveis ataques.

Proteção contra Ameaças Cibernéticas: Com a implantação de um antivírus com gerenciamento em nuvem (Kaspersky), espera-se que a organização esteja melhor preparada para identificar e neutralizar ameaças cibernéticas, como malware, ransomware e phishing.

Gestão Eficiente de Usuários: A instalação de um Windows Server com configuração do Active Directory deve melhorar o controle de acesso dos usuários e a administração de recursos. Isso deve resultar em uma gestão de usuários mais eficiente e em um aumento da segurança, garantindo que apenas usuários autorizados tenham acesso aos recursos da rede.

Backup e Compartilhamento de Dados: A implementação de um sistema de backup (OwnCloud) deve assegurar a proteção e recuperação de dados críticos da organização. Além disso, o OwnCloud permite o compartilhamento seguro de arquivos, melhorando a colaboração interna.

Atualização para um Sistema Operacional Mais Seguro: A atualização dos sistemas operacionais de Windows 7 para Windows 10 deve melhorar a segurança, uma vez que o Windows 10 oferece recursos de segurança aprimorados e suporte mais atualizado.

Conformidade com a LGPD: A implementação de uma política de segurança baseada na Lei Geral de Proteção de Dados (LGPD) deve garantir que a organização esteja em conformidade com as regulamentações de privacidade de dados. Isso inclui o tratamento adequado de informações pessoais, a notificação de violações de dados e a proteção dos direitos de privacidade dos indivíduos.

4.4 RESULTADOS OBTIDOS

Com a implementação bem-sucedida das medidas de segurança cibernética, nossa organização alcançou uma postura mais robusta e resiliente em relação à proteção dos ativos de TI e dados críticos. As ferramentas e políticas de segurança agora estão operando de maneira eficaz, contribuindo para um ambiente de TI mais seguro e confiável.

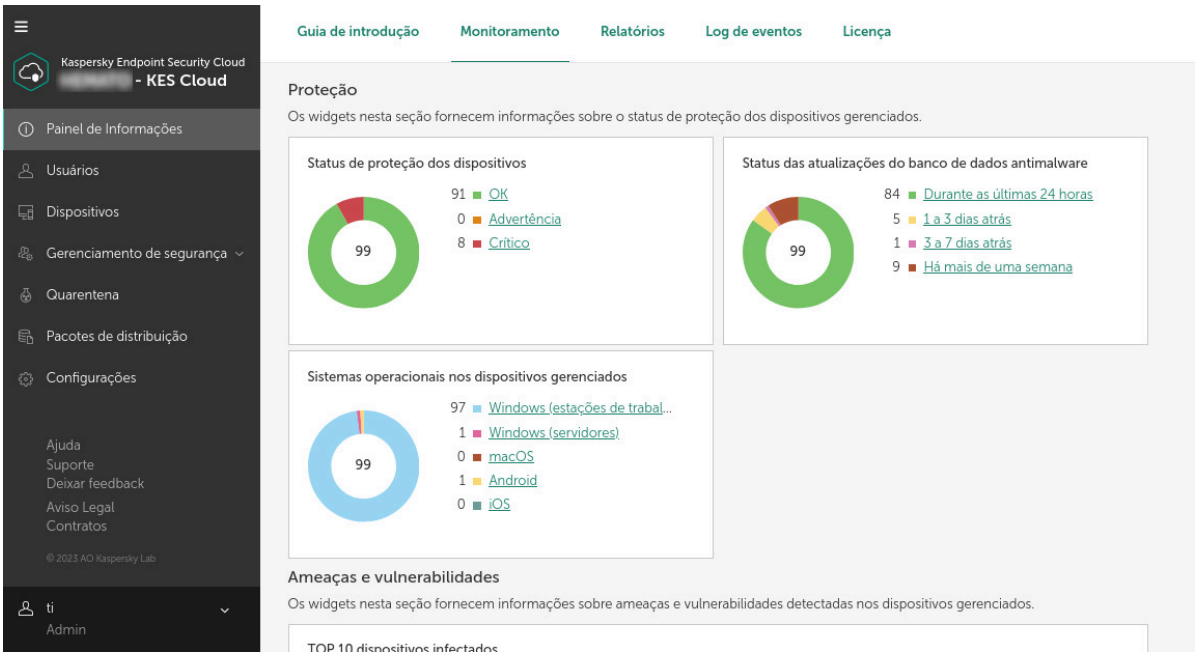

Figura 5: Antivirus Kaspersky Endpoint Security Cloud

Fonte: Autoria própria

O Kaspersky Endpoint Security Cloud proporciona resultados notáveis na defesa contra ameaças cibernéticas. Com monitoramento eficiente, detecção avançada, alertas em tempo real e atualizações automáticas, o antivírus garante uma proteção abrangente para todos os ativos da rede. Na figura 5 é possível visualizar a tela de monitoramento, pois seu controle centralizado simplifica a administração e oferece relatórios detalhados. Os resultados obtidos destacam a eficácia dessa solução na resposta proativa e na mitigação dos riscos fortalecendo a segurança digital da infraestrutura.

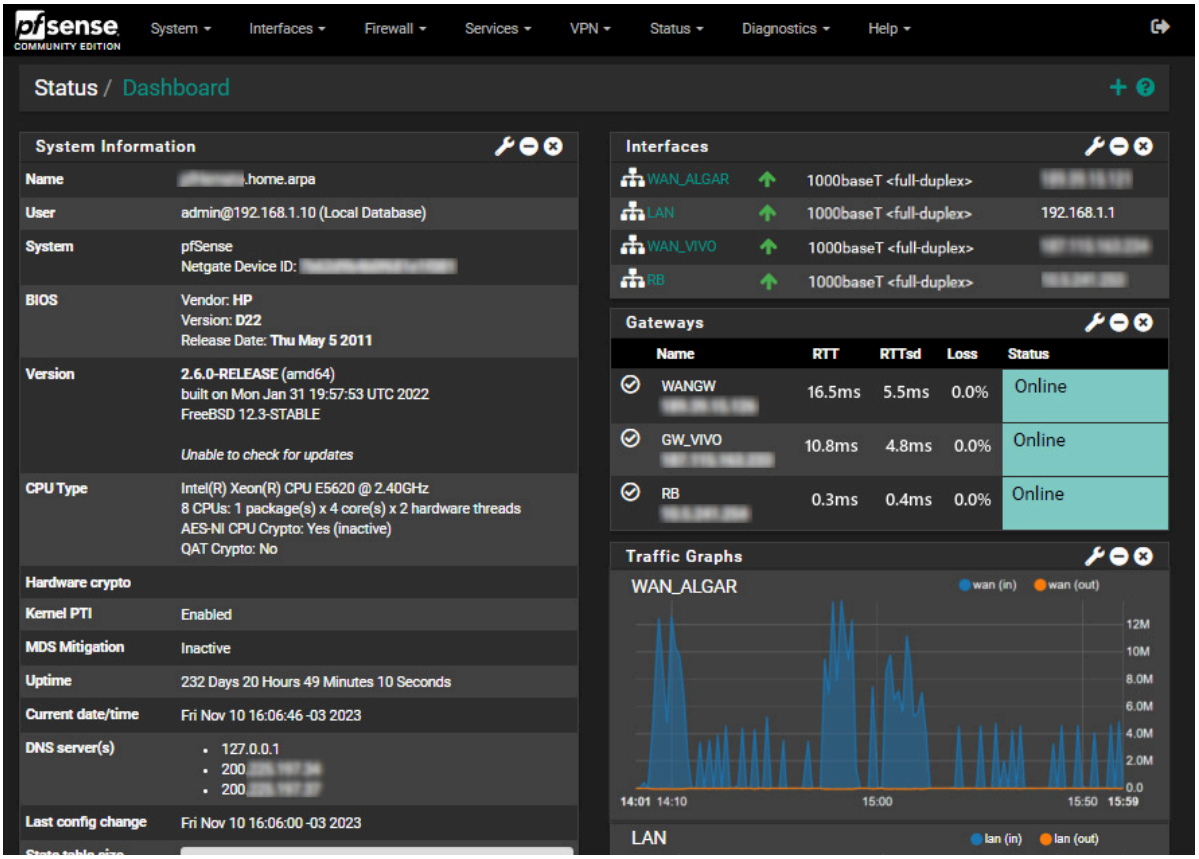

Figura 6: Sistema Firewall pfSense

Fonte: Autoria própria

Na figura 6 temos o *dashboard* do pfSense, esta ferramenta demonstrou resultados expressivos ao possibilitar o bloqueio efetivo de URLs não autorizadas, permitindo apenas o acesso a recursos previamente autorizados. Além disso, a implementação bem-sucedida dos serviços de IDS e IPS revelou sua eficácia ao bloquear endereços IPs de possíveis bot hackers, contribuindo significativamente

para a segurança da rede. Esses resultados ressaltam a capacidade do pfSense em reforçar as defesas digitais e mitigar potenciais ameaças cibernéticas.

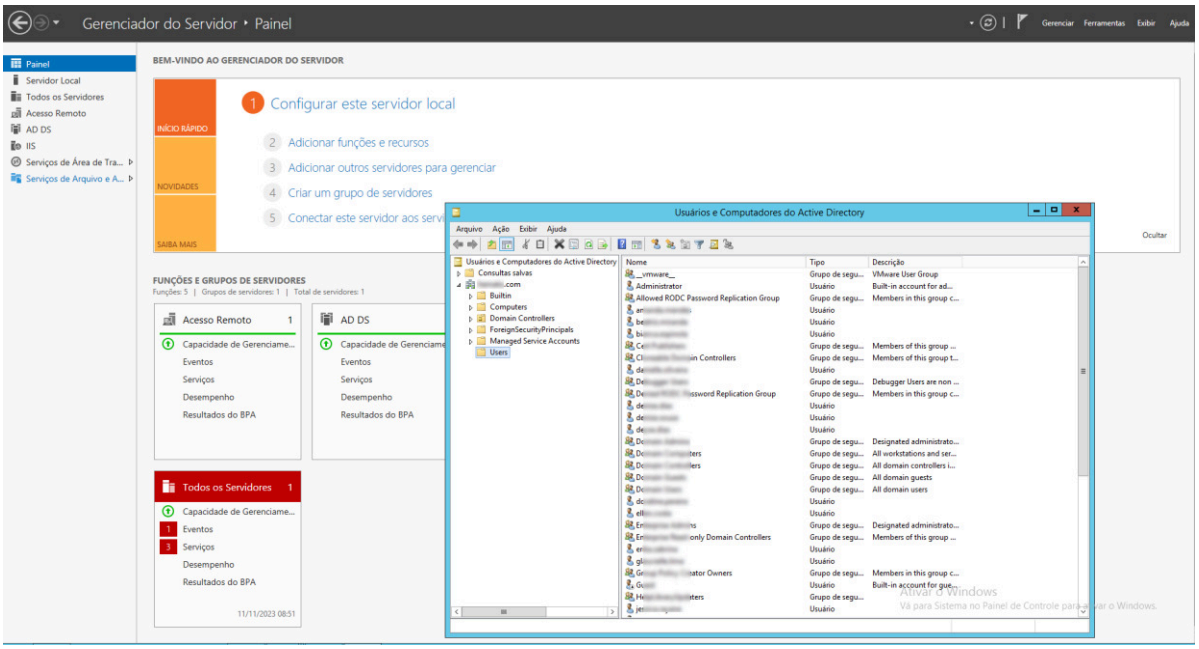

Figura 7: Windows Server 2016 - Active Directory

Fonte: Autoria própria

O sistema de controle de usuários, baseado no Active Directory (figura 7), está garantindo o acesso adequado aos recursos e as políticas de acesso estão sendo aplicadas consistentemente, fica claro identificar que apenas usuários autorizados têm acesso a informações sensíveis e isto fortalece nossa segurança e protege nossos ativos críticos.

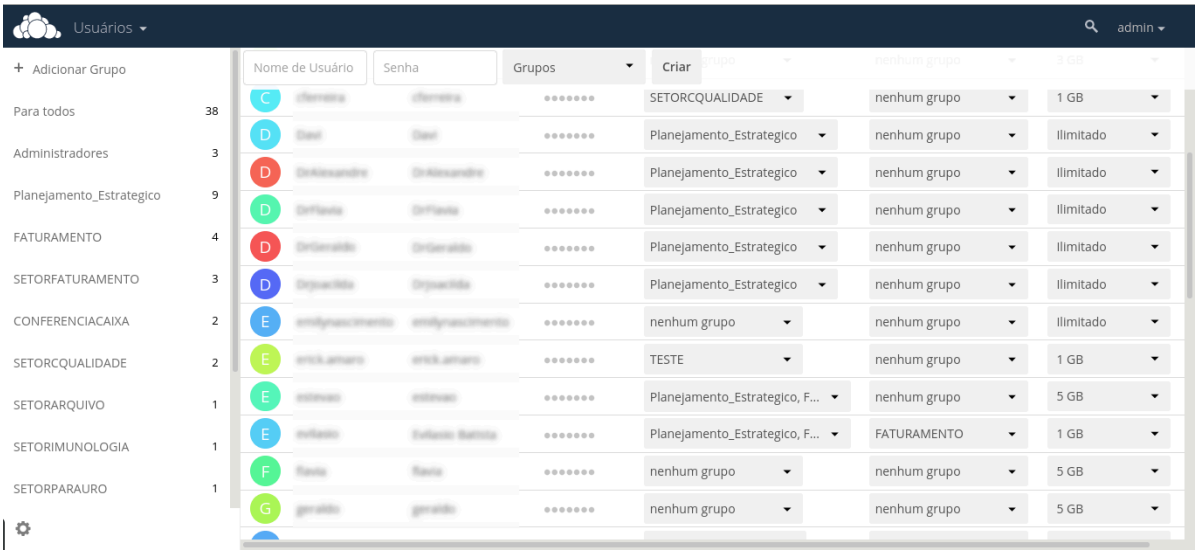

Figura 8: Sistema OwnCloud

Fonte: Autoria própria

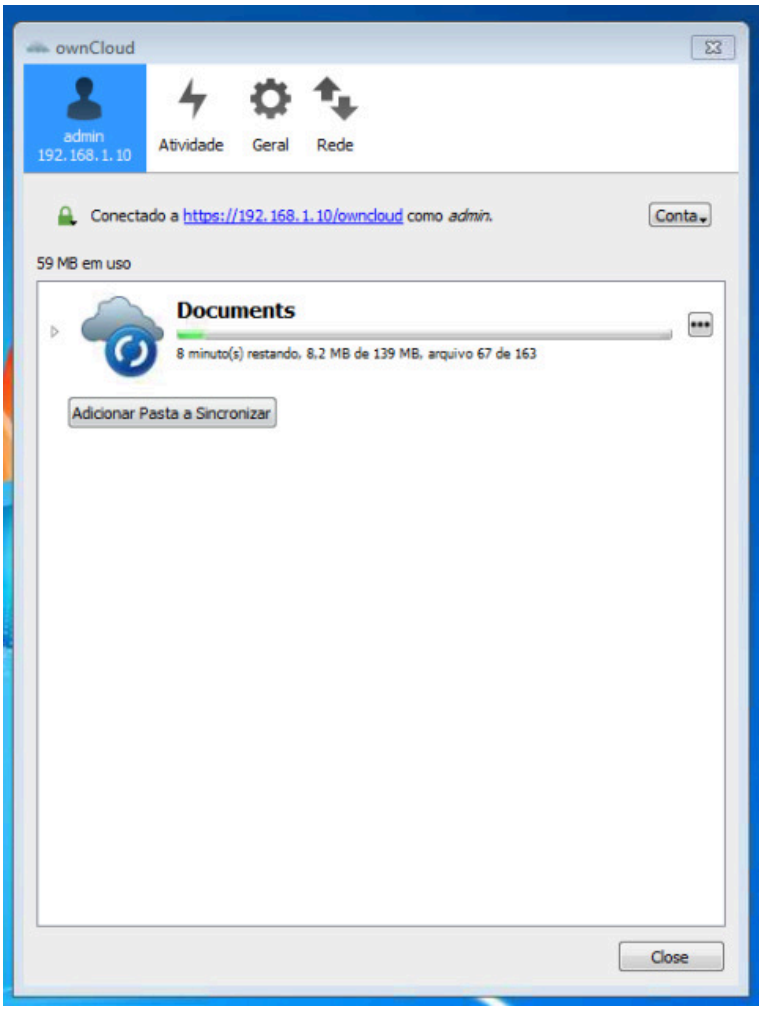

Figura 9: Agente de sincronização OwnCloud

Fonte: Autoria própria

Na figura 8 temos o painel de usuários, e na figura 9 o software Agente de sincronização. O sistema de backup OwnCloud mostrou sua eficácia por meio de testes bem-sucedidos de recuperação de dados. Foi possível verificar a praticidade de restaurar os arquivos do usuário quando há necessidade de substituir algum *desktops* obsoletos. Já nos servidores, é possível verificar diariamente que os backups estão sendo realizados para seus destinos. Estamos confiantes de que, em caso de falhas ou incidentes, nossos dados podem ser restaurados de forma confiável, minimizando a perda de informações.

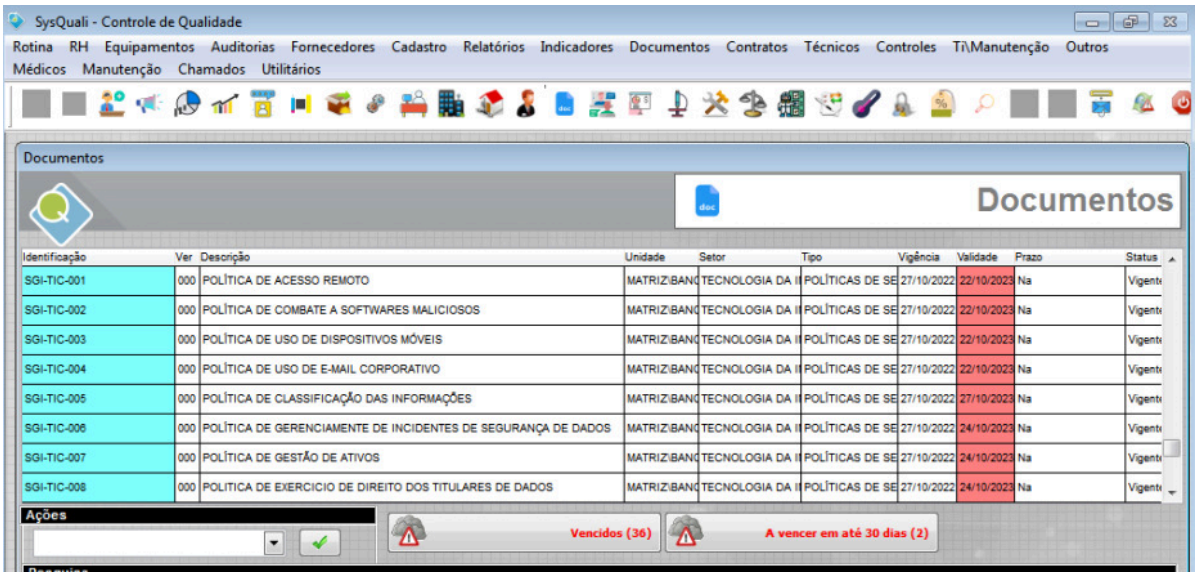

Figura 10: Sistema SysQuali - Políticas LGPD

Fonte: Autoria própria

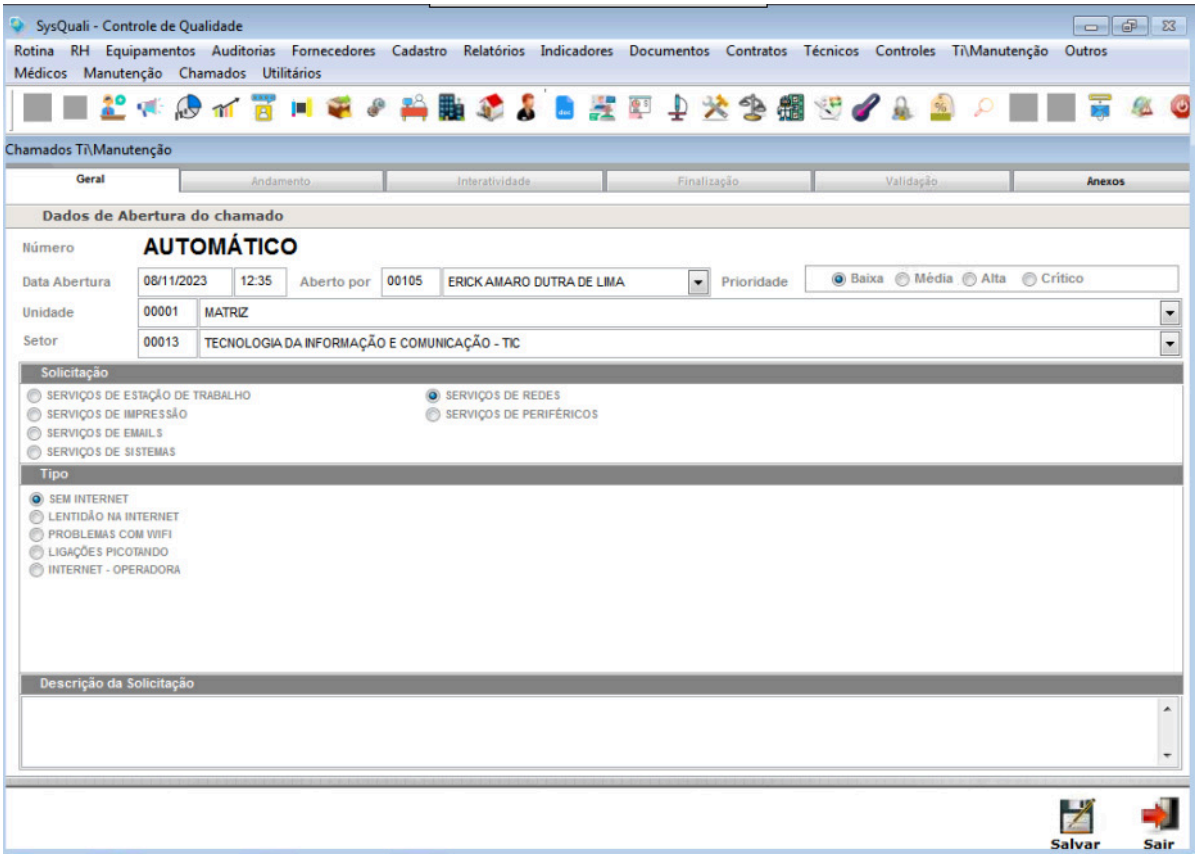

Figura 11: Sistema SysQuali - Gerenciamento de incidentes

Fonte: Autoria própria

As políticas de segurança baseadas na LGPD foram incluídas no sistema de controle de qualidade(SysQuali - figura 10 e 11) para ciência de todos os colaboradores, além disso, no próprio sistema é possível realizar o gerenciamento de incidentes(figura 11). Essas medidas essenciais asseguram os devidos cuidados exigidos pela LGPB com as informações pessoais.

Além disso, nossos funcionários demonstraram um alto nível de conscientização em relação às políticas de segurança e às melhores práticas. O treinamento contínuo e as iniciativas de conscientização estão acontecendo na medida do possível, contribuindo para uma cultura de segurança sólida em toda a organização.

Por fim, a atualização regular dos sistemas operacionais, incluindo a migração dos desktops do Windows 7 para o Windows 10 continua gradativamente

garantindo que nossos sistemas estejam atualizados e menos vulneráveis a ameaças de segurança desconhecidas.

No geral, as medidas de segurança implementadas estão cumprindo sua função de proteger nossos ativos de TI e garantindo a conformidade com as regulamentações de privacidade de dados. No entanto, a análise contínua e a vigilância garante que a organização permaneça resiliente e segura diante das ameaças que estão em constante evolução no ambiente cibernético.

5. CONSIDERAÇÕES FINAIS

5.1 SÍNTESE DOS PRINCIPAIS RESULTADOS E CONCLUSÕES

A implementação bem-sucedida do esquema de segurança cibernética na empresa X resultou em uma significativa melhoria na robustez e segurança do sistema. A empresa expressa grande satisfação ao constatar a eficácia das medidas adotadas para proteger suas operações e dados sensíveis. Com a aplicação de práticas como firewalls avançados, sistemas de detecção de intrusões, políticas de controle de acesso e conformidade legal, a empresa X fortaleceu sua postura de segurança, prevenindo acessos não autorizados e garantindo a proteção adequada de informações confidenciais.

Além disso, a resposta a incidentes foi aprimorada, proporcionando à empresa a capacidade de identificar e lidar eficazmente com potenciais ameaças. A satisfação da empresa reflete não apenas a implementação efetiva das políticas de segurança, mas também a consciência da importância de se manter atualizado frente às ameaças em constante evolução. Dessa forma, a empresa X pode operar com confiança, sabendo que está bem preparada para enfrentar desafios de segurança cibernética, garantindo a integridade e a continuidade de suas operações.

5.2 LIMITAÇÕES DO ESTUDO E SUGESTÕES PARA TRABALHOS FUTUROS

No processo de condução deste estudo, algumas limitações se fizeram presentes, afetando a extensão e a profundidade das análises realizadas. Essas

limitações, embora desafiadoras, oferecem oportunidades para melhorias futuras e pesquisas subsequentes.

Uma das limitações notáveis foi a dificuldade em instalar, configurar e testar diferentes sistemas de segurança cibernética. Essas etapas muitas vezes exigem ser realizadas durante horários atípicos, como noites ou feriados prolongados, quando a empresa não está em operação. A escolha dos sistemas a serem avaliados foi frequentemente baseada em pesquisas e experiências compartilhadas por colegas da área de TI. Esta abordagem é adotada devido à necessidade de manter a operação contínua da empresa e minimizar os riscos de interrupção dos serviços.

A limitação em experimentar novas ferramentas após a implantação, por exemplo, a aquisição do antivírus que foi baseada principalmente em sua reputação no mercado, o que torna inviável não renovar a licença para testar outras ferramentas enquanto o sistema estava em pleno funcionamento. As experiências com novas ferramentas geralmente só podem ser realizadas quando uma ferramenta existente não está garantindo seu desempenho conforme o esperado, o que limita a flexibilidade na exploração de outras alternativas.

Para trabalhos futuros, sugere-se a consideração de abordagens que permitam a experimentação de várias ferramentas de segurança cibernética sem comprometer a estabilidade operacional. Isso pode envolver a implementação de ambientes de testes isolados para avaliar diferentes soluções. Contudo, a coleta de dados sobre o desempenho das ferramentas em uso proporciona insights abrangentes e ajudam nas tomadas de decisões futuras.

Adicionalmente, estudos complementares podem se concentrar na análise de custo-benefício de diferentes soluções de segurança e na compreensão mais profunda do impacto das decisões de segurança nas operações da empresa. A exploração de estratégias de implementação flexíveis e atualizações contínuas de políticas de segurança, podem fornecer uma visão mais completa das melhores práticas de segurança cibernética e auxiliar na mitigação de futuras limitações.

5.3 CONTRIBUIÇÕES DO TRABALHO PARA A ÁREA DE SISTEMAS DE TELECOMUNICAÇÕES E SEGURANÇA

Realizar trabalhos que abordam a importância da segurança cibernética é fundamental na conscientização e educação dos profissionais de TI. Os cibercrimes estão em constante evolução, adotando novas técnicas e estratégias mais sofisticadas. Portanto, manter os profissionais de TI informados é essencial para enfrentar eficazmente as ameaças emergentes.

Esses trabalhos fornecem insights sobre as últimas tendências em cibercrimes, destacando os métodos utilizados pelos criminosos virtuais para explorar vulnerabilidades em sistemas e redes. Ao expor as novas técnicas, os profissionais de TI podem se preparar proativamente para mitigar riscos e implementar medidas preventivas adequadas.

Além disso, a conscientização sobre a importância da segurança cibernética contribui para a construção de uma cultura organizacional que valoriza a proteção dos ativos digitais incentivando investimentos em treinamentos contínuos e atualizações de habilidades para os profissionais de TI, garantindo que estejam sempre à frente das ameaças.

Os trabalhos nessa área também destacam a necessidade de colaboração e compartilhamento de informações entre profissionais, organizações e comunidades relacionadas à segurança cibernética. Essa colaboração é essencial para fortalecer as defesas cibernéticas em escala global.

Em última análise, ao alertar sobre os desafios constantes dos cibercrimes, esses trabalhos inspiram uma mentalidade proativa, promovem a aprendizagem contínua e capacitam os profissionais de TI a enfrentar os complexos cenários de ameaças digitais com confiança e eficácia.

REFERÊNCIAS

NERY, Carmen; BRITTO, Vinícius. **Internet já é acessível em 90,0% dos domicílios do país em 2021.** Agência de notícia IBGE. 2022. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021>.Acesso em: 01 de jan. de 2023.

How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool. The Guardian. 2018. Disponível em: <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm>. Acesso em: 10 de jan 2023

LATTO, Nica. **O que é o WannaCry?.** Avast. 2020. Disponível em: <https://www.avast.com/pt-br/c-wannacry>. Acesso em: 10 de jan 2023

HASELTON, Todd. **Credit reporting firm Equifax says data breach could potentially affect 143 million US consumers.** CNBC. 2017. Disponível em: <https://www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html>. Acesso em: 01 fev 2023

MOZELLI, Rodrigo. **Google, Amazon e Cloudflare neutralizam o maior ataque DDoS da história.** 2023. Olhar Digital. Disponível em: <https://olhardigital.com.br/2023/10/11/seguranca/google-amazon-e-cloudflare-neutralizam-o-maior-ataque-ddos-da-historia/>. Acesso em: 30 set 2023

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de computadores: das LANs, MANs e WANs às redes ATM**. Rio de Janeiro: Campus, 1995.

SOUSA, L. B. **Redes de computadores: dados, voz e imagem**. São Paulo: Érica, 1999.

CHIOZZOTO, M.; SILVA, L. A. P. **TCP/IP: tecnologia e implementação**. 2. ed. São Paulo: Érica, 1999.

TANENBAUM, Andrew S. **Redes de Computadores**.4ª Ed. Rio de Janeiro: Campus, 2003

TANENBAUM, A. S.; WETHERALL, D. J. **Redes de computadores**. 5. ed. São Paulo:Pearson Prentice Hall, 2011.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet: uma abordagem topdown**. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

COMER, D. E. **Interligação de redes com TCP/IP: princípios, protocolos e arquitetura**. 5. ed. Rio de Janeiro: Elsevier, 2006.

ROJANALA, Suraj. **What Is a Switch, Router, Gateway, Subnet, Firewall & DMZ?**.2022. CWNP. Disponível em:<https://www.cwnp.com/what-is-a-switch-router-gateway-subnet-firewall-dmz/>. Acesso em: 10 maio 2023

JESUS, Damásio. **Manual de crimes informáticos**, 1. ed. São Paulo: Saraiva, 2016.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

WENDT, Emerson; JORGE, Higor Vinicius Nogueria. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação**. 2. ed. Rio de Janeiro: Brasport, 2013.

TANENBAUM, Andrew S. **Redes de Computadores**.4ª Ed. Rio de Janeiro: Campus, 2003

WHITMAN Michael E.; MATTORD Herbert J. **Principles of Information Security**, Fourth Edition. 2012

FREDA, Anthony. **O que é uma vulnerabilidade de dia zero?.** 2021. Avast. Disponível em:<https://www.avast.com/pt-br/c-zero-day>. Acesso em: jul 2023

Inteligência Artificial (IA): Detecção de Anomalias de Rede e Combate ao Ransomware. Internationalit. 2023. Disponível em:<https://www.internationalit.com/post/intelig%C3%AAncia-artificial-ia-detec%C3%A7%C3%A3o-de-anomalias-de-rede-e-combate-ao-ransomware>. Acesso em: set 2023

NORTHCUTT, Stephen; NOVAK, Judy. **Network Intrusion Detection. New Riders.** Sams Publishing, 2002

O que é controle de acesso? Autorização X autenticação. Disponível em: <https://www.cloudflare.com/pt-br/learning/access-management/what-is-access-control/> Acesso em: set 2023

RIORDAN, Grant. **Autenticação x autorização – qual é a diferença?** Disponível em**:**https://www.freecodecamp.org/portuguese/news/autenticacao-x-autorizacao-qual-e-a-diferenca/ Acesso em: set, 2023.

Gerenciamento de incidentes em TI: saiba o que é e como fazer de maneira eficiente! Positivo Tecnologia. Disponível em: <https://www.meupositivo.com.br/panoramapositivo/gerenciamento-de-incidentes/> Acesso em: set 2023

5 motivos relevantes para manter atualizado o sistema operacional. Disponível em:<https://www.meupositivo.com.br/panoramapositivo/atualizar-o-sistema-operacional/> Acesso em: set 2023

Por que manter o Sistema Operacional Atualizado? Disponível em: <https://brasilcloud.com.br/sistema-operacional-atualizado/> Acesso em: set 2023

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus João Pessoa - Código INEP: 25096850
Av. Primeiro de Maio, 720, Jaguaribe, CEP 58015-435, Joao Pessoa (PB)
CNPJ: 10.783.898/0002-56 - Telefone: (83) 3612.1200

Documento Digitalizado Restrito

TCC

Assunto:	TCC
Assinado por:	Erick Amaro
Tipo do Documento:	Dossiê
Situação:	Finalizado
Nível de Acesso:	Restrito
Hipótese Legal:	Informação Pessoal (Art. 31 da Lei no 12.527/2011)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Erick Amaro Dutra de Lima**, **ALUNO (20151430246) DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES - JOÃO PESSOA**, em 16/10/2024 11:19:46.

Este documento foi armazenado no SUAP em 16/10/2024. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1279835
Código de Autenticação: 2d960184fb