CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA

REDES DE COMPUTADORES

MATEUS HENRIQUE FELIX DE BARROS

SILANIO DE MOURA RODRIGUES

THIAGO DO NASCIMENTO DA SILVA

GERÊNCIA DA REDE LOCAL (LAN): A NECESSIDADE DE UMA REDE SEGURA NO MEIO EMPRESARIAL

RECIFE/2021

MATEUS HENRIQUE FELIX DE BARROS
SILANIO DE MOURA RODRIGUES
THIAGO DO NASCIMENTO DA SILVA

GERÊNCIA DA REDE LOCAL (LAN): A NECESSIDADE DE UMA REDE SEGURA NO MEIO EMPRESARIAL

Trabalho de Conclusão de Curso apresentado ao Curso de Redes de Computadores, da UNIBRA, como requisito parcial para a obtenção do certificado, sob a orientação da Prof.ª. Ameliara Freire.

RECIFE/2021

B277g

Barros, Mateus Henrique Felix de

Gerência da rede local (LAN): a necessidade de uma rede segurano meio empresarial. / Mateus Henrique Felix de Barros; Silanio de Moura Rodrigues; Thiago do Nascimento da Silva.- Recife: O Autor, 2021.

33 p.

Orientador : Me. Ameliara Freire Santos de Miranda

Trabalho de Conclusão de Curso (Graduação) – Centro Universitário Brasileiro – UNIBRA. Graduação Tecnológica em Redes de Computadores, 2021.

1. Segurança de rede. 2. Segurança da informação. 3. Monitoração de sistemas. 4. Ferramentas de segurança. 5. Ameaças a rede. I. Centro Universitário Brasileiro. - UNIBRA. III Título.

CDU:004.7

MATEUS HENRIQUE FELIX DE BARROS
SILANIO DE MOURA RODRIGUES
THIAGO DO NASCIMENTO DA SILVA

GERÊNCIA DA REDE LOCAL (LAN): A NECESSIDADE DE UMA REDE SEGURA NO MEIO EMPRESARIAL

Artigo aprovado como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores, pelo Centro Universitário Brasileiro — UNIBRA, por uma comissão examinadora formada pelos seguintes professores:

_____

Msc. Ameliara Freire Santos de Miranda
Orientador

_____

Esp. João Freire Abramowicz
Examinador

_____

Msc. Jheymesson Apolinário Cavalcanti
Examinador

Recife, _____ de _____ de 2021.

NOTA: _____

Dedicamos esse trabalho a nossa família, mestres e amigos.

AGRADECIMENTOS

Agradecemos as nossas famílias, amigos e mestres que estiveram conosco ao longo dessa graduação. Agradecemos também aos nossos orientadores Ameliara, Jheymesson e João, assim como os professores Adilson e Aline que tiveram toda a paciência em nos explicar em cada orientação, como melhorar o nosso trabalho de conclusão de curso, para que este estivesse à altura do curso de Redes de Computadores, muito obrigado pelo carinho e compartilhamento de informações.

Em especial eu Thiago, gostaria de agradecer a minha esposa e ao nosso amigo Reginaldo que contribuíram em conselhos para a melhoria da escrita e metodologia do trabalho. Dedico esta obra a todos que nos acompanharam dentro da instituição como colegas de trabalho e fora dela, cada estágio realizado foi uma experiência única.

E finalizando, agradecemos a nós mesmos e a Deus, pela força de vontade e de fé em agregar a nós sabedoria, confiança, foco, força e garra para sempre querer mais conhecimento, construção de amizades e experiências novas.

“A perfeição não é atingível. Mas se perseguir a perfeição, podemos alcançar a excelência. ”

(Vince Lombardi)

SUMÁRIO

GERÊNCIA DA REDE LOCAL (LAN): A NECESSIDADE DE UMA REDE SEGURA NO MEIO EMPRESARIAL

Mateus Henrique Felix de Barros
Silanio de Moura Rodrigues
Thiago do Nascimento da Silva
Professora orientadora Msc. Ameliara Freire Santos de Miranda

Resumo: Com todo o avanço na área da tecnologia da informação existente na atualidade, muitas pessoas e organizações ainda sofrem com invasões indesejadas em suas respectivas redes. Dito isto, existe a necessidade de ter uma segurança digital ainda mais aprimorada nas empresas, que proporcione a permanência desta, na qual dificilmente eventos como invasões e vazamento de informações ocorram a rede. Neste intuito, o presente artigo tem o objetivo de demonstrar o quão importante e necessário é se ter uma rede segura nas empresas e a necessidade de se possuir um controle apropriado com um bom gerenciamento, proporcionando uma rede estável e protegida, possibilitando a segurança de dados sensíveis da empresa ou mesmo informações pessoais de clientes. Foi realizado uma pesquisa de revisão da literatura para identificar a real necessidade, de um gerenciamento de rede de forma segura, e como isso pode influenciar aos dados de organizações de forma benéfica. Para isso, se fez necessário realizar uma análise em trabalhos relacionados com o assunto proposto, buscando focar em como se possuir um bom desempenho nas redes empresarias, proporcionado também a segurança. Através da pesquisa realizada constata-se que os objetivos foram atendidos, pois foi possível identificar métodos para um bom gerenciamento da rede e de se ter uma rede segura e estável.

Palavras-chave: Segurança de rede; Segurança da informação; Monitoração de sistemas; Ferramentas de segurança; Ameaças a rede.

Abstract: With all the advancement in the area of information technology existing nowadays, many people and organizations still provided with unwanted intrusions into their best networks. That said, there is a need to have an even more improved digital security in companies, which provides a permanence of this, in which events such as invasions and information leaks rarely occur on the network. With this in mind, this article aims to demonstrate how important and necessary it is to have a secure network in companies and the need to have proper control with good management, providing a stable and protected network, enabling security of relevant data company or even personal customer information. A literature review survey was conducted to identify the real need for secure network management and how this can beneficially influence association data. For this, it was necessary to carry out an analysis of works related to the proposed subject, seeking to focus on how to have a good performance in business networks, also providing security. Through the research carried out, it appears that the objectives were met, as it was possible to identify methods for good network management and to have a secure and stable network.

Keyboards: Network security; Information security; Systems monitoring; Security tools; Threts to the network.

1 INTRODUÇÃO

Hoje em dia, com o crescimento das redes de computadores nas empresas, e com os inúmeros dispositivos conectados à rede, fica cada vez mais complicado o gerenciamento por parte do administrador. Isso ocorre pois cada vez mais este tipo de equipamento vem fazendo-se uma ferramenta essencial a todos os setores de uma empresa, sendo elas de grandes corporações, médias ou até mesmo de pequeno porte. Estima-se que o uso de computadores em pequenas empresas ao longo dos últimos anos, cresceu 30-80%, dependendo da localização e natureza do negócio (Palvia & Palvia, 1999).

Com isso mostra-se como a gerencia da segurança na rede é essencial e de extrema importância para uma empresa, uma vez que com uma má gerencia, dados pessoais ou informações confidencias podem vir a ser extraído e possivelmente expostos à internet. Possíveis invasões de *crackers* para se apropriar-se de informações digitais podem ocorrer, visto que a atitude de um *cracker* sempre é prejudicial, sabe-se que esses indivíduos com má intenções, desenvolve métodos e *softwares* para obter acessos não autorizados a arquivos pessoais e equipamentos, como servidores e *data centers* de uma empresa.

> “Existe uma grande confusão entre os termos *Hacker* e *Cracker*. Os Hackers são indivíduos que usam seus conhecimentos para benefício próprio, para trabalhar, para ajudar outras pessoas. Já os *Crackers* (*cracking*=quebra) são os “Piratas virtuais”, eles usam seus conhecimentos para violar sistemas ou redes. Com a criação dos computadores termos como esses foram surgindo para definir cada indivíduo que possuem amplo conhecimento na área de informática” (DINIZ e SILVA, 2017).

Visto que problemas com pessoas más intencionadas vem sendo cada vez mais frequente, e com o aumento de usuários conectados à internet, deve-se adotar uma boa prática/política de segurança na rede. Atualmente muitos profissionais da área da TI, estão em busca de qualificação, a necessidade atual pede que esse tipo de profissional busque mais certificações para que este seja cada vez mais preparados para assegurar e gerenciar bem essas redes (ROCHA,2015, p. 603).

Também se nota alguns problemas/riscos encontrados na segurança de redes, um desses é o uso indevido das informações compartilhadas através das tecnologias *Wireless* nos ambientes domésticos e empresariais, uma vez que, se elas não estiverem bem protegidas, um *hacker*/*crackers* pode invadi-las, usando algumas técnicas relativamente simples (MORAES, 2010, p. 191).

Forouzan (2007, p. 876) cita que “o objetivo do gerenciamento de segurança é controlar o acesso à rede baseado em uma política de segurança pré-determinada. ” Ao falar de rede, logo se pensa em algum tipo de compartilhamento, mas quando estamos falando no meio computacional, estamos querendo dizer sobre o compartilhamento de informações e recursos, que qualquer pessoa com acesso à rede, pode fazer uso dessas informações ou arquivos contidos a ela.

Hoje em dia podemos dizer que somos dependentes da informação por meio da internet, com o aumento do uso de dispositivos como celulares, *Tablets* e computadores pessoais que fazem uso padrão de comunicação, dentre muitos outros dispositivos com capacidade de se conectar-se à rede (CORRADINI; FELIX; MAINARDES; 2015, p. 2).

Por conta disso, devido a distribuição de informações disponibilizadas através da rede, devemos nos preocupar com a segurança de nossas informações, pois a quantidade de dispositivos que usamos no dia a dia, podem nos deixar expostos. Specialski (1999, p. 4) ressalta a necessidade da existência de “uma política de segurança robusta e efetiva e que o sistema de gerenciamento de segurança seja, ele próprio, seguro”.

Exatamente por esses problemas, muitos profissionais vêm se especializando na área de segurança da informação, para diminuírem o risco de ataques e possibilidades de vazamentos de informações. Dito isto, a busca pela segurança dentro da própria rede, sendo ela privada ou pública deve ser constante, pois, pessoas maliciosas buscam continuamente por falhas em sistemas de segurança, e novas técnicas de ataques para obterem sucesso na invasão e conseguirem extrair informações confidenciais ou algum arquivo com dados importantes, e assim tirarem algum proveito, principalmente financeiro (CASTRO; DOUGLAS, 2010).

1.1 Objetivo Geral

Evidenciar a importância de um gerenciamento da rede eficaz, pois com uma boa gerencia, o administrador da rede pode assim identificar, possíveis brechas de segurança, e realizar bons testes de instabilidade à infraestrutura da rede.

Cuidarmos de nossas informações pessoais e confidenciais na atualidade é essencial, ressaltamos assim, o quão positivo é para a privacidade dos usuários o uso de ferramentas como antivírus e uma boa configuração utilizada no *Firewall* em computadores das empresas, assim como o uso de sistemas de detecções e

prevenções de intrusos como o SNORT e OSSEC ids na proteção dos sistemas , também como a utilização de ferramentas como o GNS3, pois com o uso dele, é possível um monitoramento em tempo real de servidores e dispositivos de rede simultaneamente, para prevenir a indisponibilidade de serviços, proporcionando assim, uma segurança de qualidade ao usuário da rede, fazendo com que o uso do gerenciamento, seja essencial para a utilização de computadores nas empresas de forma segura.

1.2 Objetivo especifico

- Analisar e fazer estudos de pesquisas relacionados ao tema escolhido;
- Mostrar como um bom gerenciamento da segurança na rede, e o uso de ferramentas de proteção seja essencial para o sistema das empresas, oferecendo assim, segurança e privacidade aos usuários;
- Apresentar soluções e prevenções, contra a invasão de c*rackers*, sugerindo que seja feita uma gerencia da rede de qualidade e o uso de ferramentas de segurança no meio organizacional ;
- Mostrar como a gerência de segurança de redes, é de extrema importância para assegurar o sistema de redes e computadores de uma empresa.

2 METODOLÓGIA

A metodologia utilizada foi baseada em revisão de pesquisa bibliográfica, tomando como base a leitura de livros reconhecidos da área de segurança em redes e acesso a sites reconhecidos da área de segurança, que foram selecionados com base em pesquisas realizadas através da Internet e recomendações de profissionais da área de segurança. Inicialmente foram selecionados livros, revistas, artigos e anais, publicações avulsas ou impressas em sites e foi realizada uma análise do conteúdo pertinente ao assunto.

Foram encontrados entre livros, revistas e pesquisas no Google Acadêmico e no Science 47 referências de autores, porem fizemos o uso do texto de 32 que corroboravam com o tema, os outros 16 não falavam sobre a área de segurança em redes, ou proferiam, mas não conseguiram agregar mais informações a essa

pesquisa, uma vez que os mesmos já diziam sobre as mesmas coisas ou articulavam sobre um tema diferente.

Este trabalho definisse por caráter qualitativo, uma vez que busca trazer qualidade para o gerenciamento da rede nas empresas, melhorando os sistemas de proteção, mostrando assim, como a utilização de antivírus e sistemas de bloqueios nas empresas podem impedir o vazamento de dados de seus clientes, assim como dados sensíveis próprios da organização. Ressaltamos que foram utilizados textos recentes e antigos, para que a pesquisa tivesse uma amplitude maior, com a visão de vários autores de épocas diferentes a atual e o que eles já produziam sobre temas como a tecnologia e sobre a melhora da segurança e da rede.

Alguns autores citados são TANENBAUM sobre redes de computadores (2003); FOROUZAN que foi citado sobre a comunicação de dados e redes de computadores (2006) LOPES e NICOLLETTI falando sobre Melhores Práticas para Gerência de Redes de Computadores (2003), como autores antigos. E Diniz que fez um estudo sobre *hacker e cracker:* Um estudo sobre suas diferenças e os crimes virtuais (2017) e também MACHADO que escreveu sobre o sistema de informação e gestão de tecnologia 2 (2019) como temas recentes.

3 REFERENCIAL TEÓRICO

3.1 Segurança da Informação

A segurança da informação é um dos tópicos de mais importância dentro das organizações em função do grande número de ataques virtuais, realizados por ciber-criminosos no mundo todo, pois, ataques a empresas vem aumentado a cada dia que passa. SPANCESKI (2014, p. 41) define segurança da informação como " uma área de conhecimento voltada à proteção da informação e dos ativos associados contra indisponibilidade, alterações indevidas e acessos não autorizados."

Segundo a TECHNET (2006) – órgão responsável pela manutenção da Academia Latino-americana de Segurança da Informação, pertencente a Microsoft Corporation –, os pilares da Segurança da Informação abordados pela ISO 17799:2000 – padrão internacional específico para segurança da informação –, são: Disponibilidade, Integridade e Confidencialidade.

3.1.1 Confidencialidade

MACHADO (2019, p. 298) diz que “A confidencialidade é a propriedade da informação de se manter acessível aos agentes autorizados e, ao mesmo tempo, inacessível aos agentes não autorizados. ” Portanto, a confidencialidade resulta na proteção dos dados privados da organização, ela tem por interesse proteger informações que são repassadas a essa empresa e que são garantidos em oferta que serão mantidos em sigilo, pois se um serviço é contratado por uma empresa a confidencialidade é levado em questão em primeiro lugar, pois nenhuma empresa quer que seus dados confidenciais sejam vazados.

Desta forma, a confidencialidade tem a ver com a privacidade dos dados da organização, ações por parte dos administradores da rede na empresa, devem ser tomadas para assegurar que informações críticas, sendo elas confidenciais ou pessoais não venham a ser extraídas e consequentemente roubadas dos sistemas organizacionais por meio de ciber-ataques, espionagem, entre outras práticas realizadas por pessoas más intencionadas.

3.1.2 Integridade

Conforme (MACHADO, 2019):

> A integridade é a propriedade da informação de se manter sob controle e poder ser alterada por agentes autorizados e, ao mesmo tempo, impedida de sofrer alterações por agentes não autorizados (MACHADO M. p. 298).

Sendo assim, a integridade tem por precisão, consistência e confiabilidade das informações e sistemas da empresa ao longo dos processos ou de seu ciclo de vida, pois os dados armazenados devem estar no mesmo modo de armazenamento em que foram criados, para se ter a certeza que são os mesmos arquivos. Por vez, o transporte desses dados por meio da rede pode vir a ser corrompidos ou interceptados pessoas má intencionadas conectadas à rede, assim podendo ser alterados facilmente por pessoas que trabalham ou não na empresa mesmo antes de chegarem ao destinatário.

É de extrema importância que os dados e informações circulem ou sejam armazenados do mesmo modo como foram criados, sem que tenha ocorrido nenhuma interferência externa para alterá-los ou corrompe-los. Uma forma de garantir a

exatidão da informação, é de se estipular controles de acesso a certas áreas do sistema, como pastas e arquivos para os usuários da organização, que não seja os próprios administradores, assim como definir permissões de arquivos e usar sistemas de verificação para detectar alterações nos dados (SARDENBERG,2015).

3.1.3 Disponibilidade

Ressaltamos que um dos pontos chave buscados pelas empresas, é o fácil acesso as suas informações, para as empresas, se torna crucial que suas informações possam ser acessadas por elas a qualquer momento, sem que lhes ocorra algum empasse na obtenção de seus dados, para MACHADO (2019) a disponibilidade é “a propriedade da informação de se manter acessível a agentes autorizados a qualquer momento que se precise dela. ”

Posto isso, esse princípio está diretamente relacionado à eficácia do sistema e do funcionamento da rede, para que assim, as informações e dados sejam acessados sem que tenha algum problema de comunicação no momento do acesso. Portanto, para garantir a disponibilidade da informação, é preciso uma estrutura construída de forma adequada e uma gerencia de recursos por parte da empresa.

3.2 Gerenciamento de redes

Segundo CORDEIRO (2016, p. 6) “Gerência de redes é o controle de todos os equipamentos, seus respectivos recursos presentes em uma estrutura de rede, sendo equipamento passivo ou ativo. ” O gerenciamento da rede é uma prática de extremamente importante para empresa, pois através dela, é possível identificar possíveis brechas de segurança, assim como realizar testes de instabilidade à rede e da infraestrutura usada na empresa a fim de melhorar a segurança e a qualidade da rede. O monitoramento não é o único recurso, porém é o um dos mais importante, organização é outro fundamento considerável que essa prática possibilita, já que o administrador da rede em questão é capaz de receber informações de forma imediata em seu computador, além de poder prestar auxílio aos usuários da rede com a uma assistência técnica de maneira remota.

Para MEDRADO (2018, p. 11) o objetivo da gerência de redes é “monitorar e controlar os elementos da rede (sejam eles físicos ou lógicos), assegurando um

certo nível de qualidade de serviço.” Para realizar esta função, os administradores da rede são geralmente auxiliados por um sistema de gerência de redes contendo um acervo de ferramentas integradas para a monitoração e controle da rede. Não existe no mercado sistemas que oferecem um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas de limpeza da rede (STALLINGS, 1998 apud LOPES; SAUVE; NICOLLETTI, 2003, p. 17).

3.3 Gerenciamento de Ativos

Segundo TANENBAUM (2011) “ativos são todos os componentes da rede que criam, processam, armazenam, transmitem ou descartam dados. ” Sendo assim, os ativos de redes são todos os equipamentos utilizados na infraestrutura como switches, repetidores, concentradores, roteadores, bridge, modem, gateway, adaptadores de rede, firewall, pontos de acesso sem fio, dentre outros hardwares.

No gerenciamento de ativos é interessante dedicar-se e focar nos equipamentos que possui maior importância na infraestrutura, sendo esses os responsáveis pelo processamento da rede e armazenamento de dados, tal como, o gerente e o agente e os *data-centers*, que são importantes e devem ser tratados com prioridade para qualquer tipo de rede. Um conjunto de métodos e procedimentos no uso da VLAN (*Virtual Local Area Network*) VTP (Vlan *Trunking Protocol*) e STP (*Spanning Tree Protocol*) permitem que seja empregado uma a maior performance para todo o sistema e uma ótima eficácia a os recursos presentes a ativos de rede, recursos esses que podem ser aplicados entre o usuário final, e a parte administrativa da rede onde estão presentes os servidores (ODOM, 2008 p. 490).

3.4 Segurança de rede

Segurança de rede é qualquer atividade projetada para proteger o acesso, o uso e a integridade da rede corporativa e dos dados (CISCO ,2021).

- Inclui tecnologias de hardware e software;
- Tem como alvo uma variedade de ameaças;
- Impede que as ameaças entrem ou se espalhem na rede;
- A segurança eficaz da rede gerencia o acesso à rede.

Segura de rede serve para a proteger as redes de uma determinada empresa, criando o impedimento de atividades ou acessos que não são autorizados, seu objetivo é proteger os dados e os alicerces da rede impedindo ameaças externas. Devido a migração dos aplicativos corporativos para as nuvens públicas, se faz necessário que esses aplicativos sejam distribuídos para várias áreas, consequentemente algumas dessas áreas ficam fora do controle físico das equipes de segurança de TI.

A ideia é transformar uma rede simples sem segurança, por uma de alto nível e segura, para que assim a rede possua mais áreas de defesas e que as soluções possam ser automatizadas e tenham uma maior dimensão. A utilização de ferramentas e mecanismos de segurança é extremamente importante, pois com soluções como essas, a privacidade e os dados de uma empresa estarão sempre seguras, evitando assim a captura ou vazamento de dados e informações.

3.4.1 Política de Segurança

Conforme RAVANELLO (2004, p. 21) existe uma fronteira virtual erguida pelas entidades na forma de sua política de segurança, conforme isso “uma política de segurança é um conjunto de regras que visa regulamentar a produção, acesso e tráfego de informações e recursos computacionais em uma organização e determinar formas de agir em caso de violação destas regras. ” A Junção dessas regras, são usadas como limitador para definir o escopo das técnicas e ferramentas de segurança de uma rede.

A política de segurança de uma empresa é, provavelmente, o documento mais importante em um sistema de gerenciamento de segurança da informação, o proposito que se pretende alcançar é de se normatizar as práticas e procedimentos de segurança da empresa. Uma das melhores formas de se prevenir contra invasões, é de se gerar e respeitar uma política de segurança que engloba atualização de softwares, controle de recursos disponibilizados na rede e acesso físico ao sistema, o controle de senhas e pelo uso de ferramentas de proteção de sistemas como Firewalls e IDS´s (SPANCESKI, 2004).

3.4.2 Firewall

Segundo GONÇALVES (1998, p. 2) “Um *firewall*, ou filtro de pacotes, é um recurso utilizado para proteger uma máquina ou uma rede através do controle e filtragem dos pacotes/datagramas que entram ou que saem ” com a utilização do firewall, é possível criar regras para se ter controle da rede, fazendo ele uma barreira de proteção contra acessos de conteúdos maliciosos.

Basicamente, uma regra é a definição do tipo de pacote, cada tipo de regra aceita uma coleção de ações possíveis, o administrador da rede pode rejeitar, aceitar, modificar, registrar, ignorar, marcar pacotes ou até mesmo fazer com que os pacotes sejam avaliados de acordo com outros conjuntos de regras, permitindo que pacotes de dados compatíveis com estas regras passem enquanto todos os outros nunca cheguem ao seu destino final.

É comum a utilização de *firewalls* baseados em *hardwares* em empresas, a grande vantagem da utilização destes, é que eles são *hardware* totalmente dedicados a proteção, não compartilhando recursos com outros tipos de aplicações, dessa forma é possível que ele trabalhe nas proteção e requisições de forma mais ágil. Estes equipamentos especializados. O firewall é apenas uma de muitas ferramentas que devem ser usadas para se ter uma segurança de qualidade em uma rede, sendo assim, não deve ser a única a ser usada para proteger o sistema.

3.4.3 IDS/IPS e IDPS

Tomando como base o que HOCK e KORTIŠ (2015) explicam:

- IDS

É um sistema de detecção de intrusão (*Intrusion Detection System*), sendo um software que automatiza o processo de detecção de intrusão, ele monitora o tráfego de dados, avisa sobre ataques e tentativas de intrusão e pode verificar se uma ação é ameaçadora ou não. O IDS também, fornece proteção adicional para os ativos de rede de uma empresa.

- IPS

Um sistema de prevenção de intrusão (*Intrusion Prevention System*) é um software de prevenção de intrusão. Tem a capacidade de impedir possíveis incidentes. Com isso, Além de identificar uma invasão, ele t também é capaz de

explorar qual a parcela de risco dela e bloqueá-la imediatamente caso necessário. Seu funcionamento restringe-se em enviar avisos ao administrador da rede por meio de alarmes se houver algum acesso não autorizado. Com isso ele pode redefinir a rede em casos como este, ele derruba pacotes maliciosos e bloqueia o tráfego.

- IDPS

Um Sistema de Detecção e Prevenção de Intrusão (*Intrusion Detection and Prevention System*) é um sistema híbrido, surgido a partir da junção dos sistemas IDS e IPS. É possível ainda que o administrador da rede desative as funções de IPS, fazendo assim, que o sistema funcione apenas como IDS.

3.4.4 Snort

O Snort é um Sistema de Prevenção de Intrusão *open-source*, sendo este, um dos mais importante do mundo. Segundo o próprio site do SNORT (2021) “O Snort IPS usa uma série de regras que ajudam a definir a atividade de rede mal-intencionada e usa essas regras para encontrar pacotes que correspondam a eles e gerar alertas para os usuários. ”, sendo ele baseado em rede, este sistema é capaz de detectar quando um ataque está sendo realizado, ele também consegue mudar suas configurações baseadas no ataque que esteja ocorrendo, funcionando assim, como um híbrido de IDS com IPS, formando um IDPS.

3.4.5 Ossec ids

Conforme o site OSSEC (2021) “OSSEC tem um poderoso mecanismo de correlação e análise, integrando análise de log, monitoramento de integridade de arquivo, monitoramento de registro do Windows, aplicação de política centralizada, detecção de *rootkit*, alerta em tempo real e resposta ativa ” sendo este, um *software* de código aberto.

Com o OSSEC é possível o monitoramento dos dados usando a detecção de intrusão baseada em registro em tempo real, ele contém também resposta ativa, sendo possível responder a ataques e mudanças no sistema. Ele consegue realizar um inventário do sistema, coletando informações como o *hardware* usado e os *softwares* instalados, serviços de rede dentre outras informações.

3.4.6 VPN

Conforme explica FERGUSON (1998):

> Uma VPN é um ambiente de comunicação no qual o acesso é controlado para permitir conexões de mesmo nível apenas dentro de uma comunidade de interesse definida, e é construído através de alguma forma de partição de um meio de comunicação subjacente comum, onde este meio de comunicação subjacente fornece serviços à rede sem exclusividade.

Sendo assim, uma VPN (*Virtual Private Network*) é uma rede privada virtual de comunicações construída sobre uma rede de comunicações pública. O estimulo para o uso desta, é a privacidade das comunicações e de dados contidos na rede mediante a outras, portando, a comunicabilidade dentro de um ambiente é isolada de todos os outros que compartilham a mesma planta subjacente.

Há também diferentes tipos de VPN's, as mais comuns são: VPN PPTP sendo baseada em *Point-to-Point*, ela cria um túnel e captura os dados; VPN Site a Site ela é usada principalmente em operações corporativas, elas criam uma ponte virtual que liga redes em vários lugares diferentes, para conectá-los com a Internet e manter uma comunicação segura e privada entre essas redes; IPsec tem o encargo da proteção à comunicação do protocolo de Internet, analisando cada sessão e criptografando individualmente os pacotes de dados em toda a conexão; SSL e TLS as duas são utilizadas para a criação de uma VPN, a qual o navegador é tratado como cliente e o acesso de usuário é restringido a aplicativos específicos em vez de toda uma rede, é utilizado principalmente por sites de compras online e prestadores de serviços; dentre alguns outros.

3.4.7 Antivírus

Conforme SAWAYA (2002, p. 26) diz, " um programa para detecção e remoção de vírus em computadores. " Posto isto, eles são programas usados para proteger e prevenir computadores e outros aparelhos contra códigos maliciosos, *worms* ou vírus, com intenção de dar mais segurança ao usuário. Há alguns tipos de antivírus, o do tipo preventivo, que tem como função de prevenir que a ameaça adentre no sistema, avisando antecipadamente uma possível infecção; já os do tipo indicadores, funciona identificando programas e códigos infecciosos que podem vir a afetar o sistema, rastreando sequencias de códigos especificas associados a esses vírus;

existe também os descontaminadores, que tem como especialidade descontaminar os sistemas contaminados pela infecção de vírus e programas maliciosos.

Hoje em dia tornou-se comum a junção dessas funções em um único antivírus, sendo possível a realização de uma configuração para que se tenha varreduras automáticas ou manuais no sistema de arquivos a procura desses códigos ou *softwares* mal-intencionados, ele também fica ativo 24 horas por dia protegendo o usuário contra essas ameaças e assim que encontrados excluídos do sistema (GCFGLOBAL, 2021).

3.4.8 ZABBIX

Zabbix é um software de *open-source*, ou seja, disponível abertamente, com ele é possivel monitorar constantemente a capacidade de resposta dos serviços, com base em sua conexão e a qualidade do hardware de conectividade ativo. De acordo com Olups (2010), o Zabbix oferece muitas opções para monitorar vários aspectos da infraestrutura de TI. Pode ser caracterizado como um sistema de monitoramento parcialmente distribuído com gerenciamento centralizado. Embora muitas instalações tenham um único banco de dados central, é possível usar monitoramento distribuído com nós e proxy, e a maioria das instalações irá usar agentes Zabbix.

3.4.9 Wireshark

De acordo com LAMPING, Ulf; WARNICKE (2004, p. 1) “O Wireshark é um analisador de pacotes de rede. Um analisador de pacotes de rede tentará capturar pacotes de rede e tenta exibir os dados do pacote tão detalhados quanto possível. “ Sendo assim, possível para o administrador da rede, ou até mesmo um intruso, a qual consiga uma conexão com uma rede sem boas proteções, visualizar o tráfego de pacotes, permitindo, em alguns casos, a captura destes, para analisar de forma detalhada cada um, como, por exemplo, pacotes do tipo HTTP GET, que possuem informações de *login* como nome de usuário e senha em determinados sites da web.

3.4.10 Netwox e Netwag

Netwag (DAMALIO, 2008) é a versão gráfica do antigo Netwox, sendo mais fácil localizar e utilizar as ferramentas. O Netwag executa procedimentos em janelas

ou em linhas de texto e guarda o histórico de comandos utilizados. Ele tem várias funções, desde "*sniffer* " de pacotes de dados até "*spoofe*r" informações em uma rede. Também executa testes relevantes para o bom desempenho da rede e para validar a segurança da mesma. Além de que o Netwox, é uma ferramenta muito interessante para proteger e prevenir ataques à rede. Ele também detecta possíveis causas de um desempenho lento e instável da rede.

3.5 Ameaças

Ameaças são quaisquer eventos que explorem vulnerabilidades, com potencialidade de causar incidentes indesejados, resultando em possíveis danos para a organização. As ameaças podem afetar um ou vários ativos, provocando impactos que variam de acordo com o tipo e a importância do ativo afetado (ABNT NBR ISO/IEC 27005, 2011).

3.5.1 *Malwares* e vírus

Dentre os diversos tipos de ameaças e ataques digitais existentes, destacam-se os *malwares.* O termo *malware*, abrange todo software malicioso que pode ser perigoso para o seu computador, são códigos maliciosos que exploram vulnerabilidades dos usuários com a finalidade de controlar e manipular o computador da vítima, isso inclui vírus e cavalos de Troia.

Um bom exemplo de *malware* é os *ransomware*, que são códigos maliciosos que tem o objetivo de sequestrar os dados da vítima e bloqueá-los, podendo até encripitar o sistema do computador por completo, e num momento posterior, solicitar um valor de resgate. Em outras palavras, podemos definir *ransomware* como um *malware* que confisca e rouba os arquivos de um computador, e cobra resgate para que a pessoa tenha aqueles arquivos de novamente. Dependendo da importância dos arquivos, pessoas ou empresas acabam pagando para que os seus dados sejam devolvidos, mais não há nenhuma garantia para que isso venha acontecer (LISKA; GALLO, 2016).

Ransomware é um negócio que anda crescendo, pois é bastante lucrativo para quem está por traz dos ataques, a empresa kaspersky ressalta que “Um dos maiores e mais sérios ataques de *ransomware* ocorreu em maio de 2017 e se

chamou *WannaCry*. Durante o ataque, cerca de 200.000 vítimas de cerca de 150 países foram coagidas a pagar um resgate em bitcoins" (KASPERSKY,2021).

Portanto, uma vez instalado o *malware*, este poderá criptografar (ou encriptar) os arquivos mais importantes, como por exemplo, anotações pessoais, arquivos Word e Excel ou documentos de escritório com dados sigilosos, assim também como fotos em PNG ou em qualquer outro tipo de extensão, arquivos de projetos em programas como o photoshop, e até mesmo de todo o sistema operacional.
Outro exemplo são os Spyware e Trojans (Cavalo de troia):

Segundo Costas et al(2009)*,*

> *Spyware*, Spy em inglês, significa espião e foi com essa característica que os *spywares* surgiram. Ele funciona com um simples objetivo roubar informações pessoais como login e senha, em devidos casos o *spyware* também agem para a modificação de configurações do computador (como a pagina home do seu navegador). *Trojan Horse* significa (cavalo de Tróia) é um código malicioso que faz passar por outro programa qualquer e que acaba criando vulnerabilidade no computador infectado, possibilitando na maioria dos casos, a infecção deste por outros *malwares* (Costas, 2009).

Desta forma*, Spyware* é um tipo de *malware* que tem como sua principal função se esconder, pois foram projetados para ser invisíveis enquanto registra e envia secretamente informações e atividades online, realizadas em computadores de empresas ou mesmo de uso pessoal, quanto mais tempo ele fica sem ser detectado, maior poderá ser os danos. Alguns tipos de *Spyware*s também podem por exemplo ligar microfones para poder ouvir o que está sendo falado assim como uma escuta, é possível também que seja ligado a câmera do dispositivo, sem que essas ações sejam detectadas. Funções como *keylogging* (registrar tudo o que você digita, inclusive os usuários, senhas, informações bancárias, conversas etc.) são das mais preocupante.

Já os cavalos de troia podem se parecer com qualquer coisa, inclusive vários tipos de formatos de arquivo, como por exemplo arquivos de textos, seja ele .txt ou .docx, assim como um jogo de computador baixado de um site estranho dizendo ser "gratuito", até mesmo um anúncio publicitário pode tentar instalar alguma coisa no seu computador. Muitos trojans incorporam funcionalidades de *backdoors*, para que assim o atacante tenha acesso à maquinas infectadas, um *backdoor* é como se fosse uma "entrada secreta" oculta para a maioria, mais conhecida para o atacante que criou e à inseriu no sistema, para poder ter acesso ao computador e aproveitar sem ser vistos

e realizar suas ações, sendo essas, causadoras de grandes danos a vítima ou empresa aos quais estão os computadores.

3.5.2 DDoS / DOS- Ataques de Negação de Serviço

Ataques que visam causar indisponibilidade dos serviços de um determinado processo através do envio de simultâneas requisições e pacotes a um determinado alvo visando degradar a qualidade ou tornar complemente indisponíveis os serviços oferecidos pela vítima, os ataques crescem significativamente em volume, sofisticação e impacto a cada dia que se passa.

Os recursos de rede, como servidores Web, tem sucesso a atender apenas um limite finito de solicitações possíveis, que venha acontecer ao mesmo tempo a eles. Além disso, a conexão entre o servidor e a Internet também tem sua velocidade de upload e download finita, sendo assim, toda vez que o número de requerimentos de acesso ultrapassa os limites de capacidade de qualquer componente da infraestrutura, o nível do serviço tende a sofrer instabilidades ou até mesmo para de funcionar (KASPERSKY,2021).

3.5.3 Engenharia social

A engenharia social é um termo que define algumas práticas utilizadas para obter acesso a informações, por meio da quebra de sigilo em sistemas, organizações ou de indivíduos, utilizando-se de pesquisas, trapaças, ou exploração da confiança das pessoas. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) (2012, p. 115) define engenharia social como “uma técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações”, os ataques a segurança da informação por meio da engenharia social, mediante a informações e arquivos obtidos na internet, estão ficando cada vez mais avançados e complexos, sendo a engenharia social cada dia mais preocupante.

Os golpistas procuram enganar e persuadir as vítimas a fornecerem informações sensíveis ou a realizarem ações, acessar páginas falsas, baixar arquivos em e-mails, assim executando códigos maliciosos sem mesmo elas saberem. Com os dados das vítimas em mãos, os golpistas costumam realizar transações financeiras,

enviar mensagens eletrônicas se passando pelas vítimas, abrir empresas fantasmas, comprar bens com os dados pessoais e outras atividades maliciosas (CERT, 2012).

4 RESULTADO

As invasões ocorrem com muita frequência devido a exploração da vulnerabilidade da rede, com isso criar políticas de segurança mais rigorosas são cruciais para dificultar ou impedir a tentativa de invasão. Sendo assim ressaltamos a importância de conscientizar os donos das empresas sobre a necessidade da utilização de ferramentas com o intuito de proporcionar maior segurança a rede e também melhorar seu desempenho, impedindo a indisponibilidade dos sistemas, melhorando também a segurança de dados sensíveis.

Fizemos a análise dos resultados obtidos e notamos que definir quem tem acesso à rede, e qual usuário terá acesso a que determinado dado, é de extrema importância. Assim como a constante melhora dos equipamentos é sempre necessário para a segurança, da mesma maneira que configuração de novas regas e barreiras à rede, utilizando-se de ferramenta como o próprio *firewall* e equipamentos como *fortigate* e um antivírus de boa qualidade, buscando sempre soluções de segurança integrada, assim, proporcionando proteções a rede da organização contra *malwares* ou *softwares* maliciosos que podem se infiltrar no sistema, afim de causar danos ou roubar informações.

É sempre válida a utilização de VPN’s nessas redes privadas, pois com o uso destas, é aumentada consideravelmente a segurança na organização, deste modo, é possível separar e configurar a rede de cada departamento de uma empresa, isolando uma da outra, assegurando assim, os setores com maior prevalência de dados sensíveis a qual não se faz interessante que ocorra vazamentos, como por exemplo, o setor de RH e setores administrativo como também o setor financeiro da empresa.

O uso de sistemas como o de detecção de intrusão é de extrema importância, assim como o sistema de prevenção de intrusão, para que assim a rede esteja protegida. O monitoramento e teste na segurança, utilizando-se de ferramentas como o GNS3, diminui as chances de invasões e intensificam a proteção. Salientamos também, a importância da utilização de programas como o *workload* para uma boa gerencia, possibilitando gerenciar todas as interações com a rede, fazendo com que possíveis erros sejam encontrados, prevenindo a rede de um funcionamento não

esperado, por parte dos administradores, sendo essas algumas das soluções que obtivemos a partir desta pesquisa**.**

Citaremos abaixo 2 trabalhos em especifico a qual analisamos, mais para a criação dessa pesquisa, vários outros trabalhos foram analisados, com o objetivo de capturar evidencias sobre gerenciamento, segurança e monitoramento de rede. A Tabela 1 ilustra o resumo de alguns desses trabalhos analisados.

Tabela 1. Trabalhos analisados

Citação	**Título**
SOUZA, D. M., HANNA, M. W., & ACOSTA, R. B. (2020)	GERENCIAMENTO E MONITORAMENTO DE REDES COM ZABBIX
SILVA, A. T., STEIN, M. V. S., CARVALHO, W. L. G. & ACOSTA, R. B. (2020)	GERÊNCIA DE REDES: DESEMPENHO DE REDES

Fonte: autores

4.1 Ferramentas

O trabalho de SOUZA, HANNA e ACOSTA (2020) foca em sistema de monitoramento que oferece com tecnologias de gerenciamento com uma grande dependência de muitas instituições por seus serviços, aonde surge a grande necessidade de querer encontrar formas de permitir o gerenciamento de toda a infraestrutura de rede, o aumento dessas redes, tornasse difícil o gerenciamento que é realizado somente com todo o esforço humano, sendo sempre necessário à instalação de um sistema de gerenciamento integrado que monitore a rede aonde alerta os administradores sobre qualquer alteração de em todos os serviços prestados. Dentre os diferentes serviços apresentados pelos autores, o GNS3 (*Graphical Network Simulator 3*) é um exemplo de ferramenta cuja sua finalidade é demonstrar todo o monitoramento em tempo real de servidores e dispositivos de rede simultaneamente, como prevenção da indisponibilidade de serviços.

Já o trabalho de SILVA; STEIN; CARVALHO & ACOSTA (2020) apresenta o *traffic profile* ou *workload*, ele ajustar todo o parâmetro do sistema gerenciador,

identificar os erros, comparar a performance entre sistemas alternativos, possibilitando-o gerenciar todas as interações com a rede.

Em relação a ferramentas o trabalho de Belentani, L. C., Marcello, J., & Florian, F. (2018) menciona o NAGIOS, ele tem como principal intuito de aplicação de monitoramento de rede de código aberto distribuída sob a licença GPL, um papel fundamental é monitorar tanto *hots* quanto serviços alertando quando ocorrerem problemas e também quando todos os problemas são resolvidos.

Na Tabela 2 é detalhado algumas das ferramentas citadas pelos trabalhos analisados.

Tabela 2. Lista de ferramentas

Ferramentas	**Descrição**	**Citado no trabalho**
GNS3 (*Graphical Network Simulator 3*)	Ferramenta cuja sua finalidade é demonstrar monitoramento em tempo real.	SOUZA, D. M., HANNA, M. W., & ACOSTA, R. B. (2020)
ZABBIX	Software de monitoramento de código aberto e como uma das soluções mais completas disponíveis no mercado da TI.	SOUZA, D. M., HANNA, M. W., & ACOSTA, R. B. (2020)
Traffic profile ou *workload*	Uma ferramenta que ajustar o parâmetro do sistema gerenciador, identificar erros, comparar a performance entre sistemas alternativos.	SILVA, A. T., STEIN, M. V. S., CARVALHO, W. L. G. & ACOSTA, R. B. (2020)

Fonte: autores

4.2 Segurança

O trabalho de SOUZA, HANNA e ACOSTA (2020) indica a segurança como benefícios pensados para uma rede, tanto segurança física quanto segurança de dados, aonde será possível determinar que seja configurado várias ferramentas de

monitoramento e trafego de rede e outros itens importante para uma rede. A segurança é algo bastante indispensável, pois há uma grande preocupação em casos de vazamentos de dados, então neste caso, a instalação de firewalls é de suma importante. No mercado atualmente, já existem diversos sistemas aonde se possibilita ao usuário a melhor escolha de configuração para implementar sistemas e equipamentos de segurança que podem ser monitorados por diversas ferramentas.

No trabalho de SILVA; STEIN; CARVALHO & ACOSTA (2020), a segurança foi abordada de forma, que o intuito de gerenciamento, monitoramento e segurança andem sempre juntos, é fundamental para que haja essa segurança e confiabilidade no trabalho prestado por pessoas e empresas, pois tendem não possuir uma boa aceitação, até que possam comprovar que realmente a rede está segura.

5 CONCLUSÃO E TRABALHOS FUTUROS

O desenvolvimento deste trabalho consiste em evidenciar a necessidade de gerenciamento de segurança da rede que se aplicar em uma empresa, sempre focando nos aspectos essenciais, como a segurança e a privacidade. A segurança é um fator sempre primordial, à vista disso, constatamos também que muitas empresas podem vir a sofrem com invasões à suas redes, e para que esses ataques sejam impedidos, sugerimos um gerenciamento de forma adequada e uma análise detalhada da rede.

Ressaltamos ainda a importância de que as organizações aprimorem suas redes privadas, assegurando assim a privacidade de dados sensíveis da empresa, assim como a privacidade de seus funcionários. Impedir possíveis ataques a segurança da rede é muito importante, com isso, a criação de um sistema de detecção de intrusão e um sistema de prevenção de intrusão é de grande valia, assim como é aconselhável o uso do Snort (*Network Intrusion Detection & Prevention System*) ou do OSSEC IDS e programas similares, visando uma proteção à rede de ótima qualidade.

Entretanto os sistemas de detecção de intrusão até então, são complicados de ser configurado e de ser operados. De modo geral, não podem ser eficientemente usados por pessoas sem experiência, já que o processo de ajuste e posicionamento de um sistema de detecção de intrusão não é nada trivial.

O monitoramento constante da rede é essencial, visto que com ele, é possível que se tenha informações importantes e assim tomar as ações necessárias. O uso de

antivírus em cada computador da organização é uma ótima ação por parte da empresa, pois com o uso de programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, com o intuito de se ter mais segurança é substancialmente benéfico a privacidade dos usuários.

Concluímos então, que as empresas devem se conscientizar cada vez mais para a segurança de suas redes, assegurando assim, os dados sensíveis da organização e os dados privados de seus clientes. Como trabalho futuro iremos realizar a pesquisa de mais artigos científicos e biografias referentes ao tema descrito, reunindo as informações das pesquisas no site: http://redescomseguranca.wordpress.com.

REFERÊNCIAS

ABNT NBR ISO/IEC 27005. **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.** 2011. Disponível em: https://intranet.cade.gov.br/folder/files/arquivo/2018/07/36d5971bffbd671093ce8accf56a2895_43f5489ccd57165e9d2ce51b64c1aaea.pdf. Acesso em: 17 jun. 2021.

BELENTANI, MARCELLO & FLORIAN**. A UTILIZAÇÃO DE FERRAMENTAS DE MONITORAMENTO PARA A OTIMIZAÇÃO DO GERENCIAMENTO DA REDE**. 2018. Disponível em: https://doi.org/10.31510/infa.v15i2.509. Acesso em:16 jun. 2021.

CASTRO COSTA, Albert Douglas et al. **A segurança na internet e sua relação com o desenvolvimento de softwares livres**. 2010. Disponível em: http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/view/2503. Acesso em: 16 jun. 2021.

CERT; CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de segurança para internet**. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 18 jun. 2021.

CISCO. **Oque é Segurança de Rede**. Disponível em: https://www.cisco.com/c/pt_br/products/security/what-is-network-security.html. Acesso em: 12 jun. 2021.

CORDEIRO Z. **Gerenciamento de redes**. Disponível em: https://pt.slideshare.net/ZeneideCordeiro/gerenciamento-de-redes-65752358?from_action=save. Acesso em: 19 jun. 2021.

CORRADINI, FELIX, MAINARDES. **Aspectos Etiológicos da Dependência em Internet: Uma Revisão Teórica**, 2010. Disponível em: http://rdu.unicesumar.edu.br/handle/123456789/2770. Acesso em: 16 jun. 2021.

COSTAS, M.et al. **A política de segurança da informação: Uma análise da rca** 025/2009 Sicoob Credip. 2009. Disponível em: http://www.infobrasil.inf.br/userfiles/28-05-S2-2-68453APoliticadeSeguranca.pdf. Acesso em: 18 jun. 2021.

DAMALIO, Douglas Brito. **Implementação de ferramenta de autenticação de acesso para a redes em malha sem fio**. Projeto de Monografia Universidade Federal do Pará. 2008.

Diniz, H. M.; Silva, G. P. **HACKER e CRACKER: Um estudo sobre suas diferenças e os crimes virtuais**, 2017. Disponível em: https://roitier.pro.br/wp-

content/uploads/2017/02/Banca-01-HACKER-e-CRACKERUm-estudo-sobre-suas-diferen%C3%A7as-e-os-crimes-virtuais.pdf. Acesso em: 13 de jun. 2021.

FERGUSON, Paul; HUSTON, Geoff. **O que é VPN?**, 1998. Disponível em: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.7689&rep=rep1&type=pdf. Acesso em: 24 jun. 2021.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**, 3.ed, Tradução de Glayson Eduardo de Figueiredo, Porto Alegre, Bookman, 2006.

GCFGLOBAL. **O que são antívirus?**, 2021. Disponível em: https://edu.gcfglobal.org/pt/virus-e-antivirus/o-que-sao-antivirus/1/. Acesso em: 17 jun. 2021.

GONÇALVES, Roitier Campos. **Firewall**. 1998. Disponível em: https://roitier.pro.br/wp-content/uploads/2016/02/Aula-08_Firewall.pdf. Acesso em: 22 jun. 2021.

HOCK, Filip; KORTIŠ, Peter. Sistema de detecção de intrusão baseado em código aberto e comercial e design de sistema de prevenção de intrusão (IDS / IPS) para redes IP. Em: **2015 13th International Conference on Emerging eLearning Technologies and Applications (ICETA***)* IEEE, 2015.

KASPERSKY. **Ransomware: definição, prevenção e remoção**, 2021. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 18 jun. 2021.

LAMPING, Ulf; WARNICKE, Ed. **Guia do usuário do Wireshark**. Interface, v. 4, n. 6, pág. 1, 2004. Disponível em: http://download2.upload.de/software/41563/14/user-guide-a4.pdf. Acesso em: 24 jun. 2021.

LISKA, A.; GALLO, T. **Ransomware: Defending Against Digital Extortion**. [S.l.]: O'Reilly, 2016.

LOPES, Raquel V.; SAUVÉ, Jacques P.; NICOLLETTI, Pedro S. **Melhores Práticas para Gerência de Redes de Computadores**. 1 ed. Rio de Janeiro: Campus, 2003.

MACHADO M. **Information Systems and Technology Management 2**, 2019. Disponível em: https://www.finersistemas.com/atenaeditora/index.php/admin/api/artigoPDF/9173. Acesso em: 22 jun. 2021.

MORAES, A. F. de. **Segurança em Redes:** Fundamentos. 1. ed. São Paulo: Érica, 2010.

ODOM, Wendell. **CCNA ICND 2: guia oficial de certificação do Exame**. 2. ed. Rio de Janeiro, RJ: Alta Books, 2008. 490 p. ISBN 9788576081883.

OLUPS, Richards. Zabbix 1.8 ***Network Monitoring***. 1ª Ed.Packt Publishing Ltd, 2010.

Palvia & Palvia. **Um exame da satisfação de TI de usuários de pequenas empresas**, SCB Computer Technology Global IT Center 1999.

RAVANELLO; HIJAZI; RAVANELLO. **HONEYPOTS E ASPECTOS LEGAIS**, 2004. Disponível em: http://www.mlaureano.org/aulas_material/orientacoes2/puc_2003_ravanello_honeynet.pdf. Acesso em 19 jun. 2021.

ROCHA, E. C. F. **Qualificação e reconhecimento de profissionais de Sistemas de Informação**. Goiâna, Universidade Federal de Minas Gerais. 2015. p. 26-29. Disponível em: https://sol.sbc.org.br/index.php/sbsi/article/view/5867/5765. Acesso em: 11 maio 2021.

SARDENBERG, RAFAEL SCOFIELD. **Integridade e confidencialidade dos arquivos na plataforma de nuvem federada BioNimbuZ**, 2015. Disponível em: https://bdm.unb.br/bitstream/10483/13502/1/2015_RafaelScofieldSardenberg.pdf. Acesso em: 18 jun. 2021.

SAWAYA, Márcia Regina. **Dicionário de informática & Internet**. NBL Editora, 2002.

SILVA; STEIN; CARVALHO & ACOSTA**. Gerência De Redes: Desempenho De Redes**. Revista Acadêmica Alcides Maya, v. 2, n. 2, 24 jul. 2020. Disponível em: http://raam.alcidesmaya.edu.br/index.php/RAAM/article/view/213/209. Acesso em: 24 jun. 2021.

SNORT. **O que é Snort?** 2021. Disponível em: https://www.snort.org/#documents. Acessado em: 23 jun. 2021.

SOUZA, D. M., HANNA, M. W., & ACOSTA, R. B. **GERENCIAMENTO E MONITORAMENTO DE REDES COM ZABBIX**. REVISTA ACADÊMICA ALCIDES MAYA, v. 2, n. 2, 24 jul. 2020. Disponível em: http://raam.alcidesmaya.com.br/index.php/RAAM/article/view/214/210. Acesso em: 24 jun 2021.

SPANCESKI, Francini Reitz. **Política de segurança da informação – Desenvolvimento de um modelo voltado para instituições de ensino**. Monografia

do Trabalho de Conclusão de Curso em Sistemas de Informação, 2004. Disponível em: http://187.52.54.51/emmonks/seguranca2/Pratica3/exemplos/ist_2004_francini_politicas.pdf. Acesso em: 23 jun. 2021.

SPECIALSKI, Elizabeth. S. **Gerência de Redes de Computadores e de Telecomunicações**, Universidade Federal de Santa Catarina, Florianópolis, 1999.

STALLINGS, W. **Criptografia e segurança de redes**. São Paulo: Pearson Prentice Hall, 2007. ISBN 978-85-7605-119-0.

TANENBAUM, Andrew S. **Redes de Computadores**. 4.ed. ed. Rio de Janeiro: Campus, 2003. ISBN.

TECHNET, M. **Curso Básico de Segurança da Informação**. Microsoft Corporation, EUA, módulo 1 edition, 2006.