OS SISTEMAS EMBARCADOS COMO PRODUTOS DE DEFESA: O EMPREGO DE FIREWALL EM INFRAESTRUTURAS CRÍTICAS EM PROL DA DEFESA CIBERNÉTICA.

TEN LUCAS CAVALLARE RUELA
TEN VINICIUS RODRIGUES ANDRADE

RESUMO: A Estratégia Nacional de Defesa de 2008 (END) definiu três setores fundamentais para a Defesa Nacional: o nuclear, a cargo da Marinha do Brasil; o espacial, a cargo da Força Aérea Brasileira; e o cibernético, a cargo do Exército Brasileiro (EB). O presente trabalho tem como objetivo principal uma análise do uso de Firewall em Hardware verificando suas possibilidades em prol da defesa cibernética, avaliando sua eficácia contra ataques cibernéticos em Infraestruturas Críticas. Recentemente observamos problemas como o aumento de ciberataques em infraestruturas críticas. Invasões a órgãos governamentais, companhias de energia elétrica e hospitais, por exemplo, tornam-se comuns com o emprego de ransomwares por parte de hackers, com o intuito de receber um valor em moeda digital em troca da chave que pode descriptografar os dados “sequestrados”. O propósito deste trabalho é alertar gestores de Infraestruturas Críticas com vulnerabilidades em segurança cibernética quanto à gravidade do assunto e fornecer uma possível solução em Hardware de Firewall em alicerce às demais ferramentas de segurança como o uso de IDS/IPS, antivírus e backup. A metodologia utilizada durante as pesquisas foi o método da revisão bibliográfica, tendo como base pesquisas documentais, sites na Internet, artigos e teses. Como resultados, o presente trabalho observou que os gestores de Infraestruturas Críticas, os quais atribuem maior relevância aos meios de defesa cibernética, foram menos suscetíveis aos diversos tipos de ataques. Concluímos, pois, que o uso de um Hardware especificamente com a função de Firewall pode gerar uma segurança adicional, bem como evitar prejuízos às empresas, infraestruturas críticas e governos.

Palavras Chaves: FIREWALL, INFRAESTRUTURA CRÍTICA, DEFESA, SISTEMA EMBARCADO.

1 INTRODUÇÃO

Na era do conhecimento e da informação, a noção de soberania de um país vai além da proteção de suas fronteiras, passa também pela capacidade deste em proteger suas organizações, informações cibernéticas e tecnologias.

A importância da proteção de informações sensíveis e segurança cibernética foi percebida no Brasil em 2008, com a criação da Estratégia Nacional de Defesa (END), cuja responsabilidade pela defesa cibernética foi atribuída ao Exército Brasileiro (EB).

Além da segurança cibernética foram definidos mais dois setores estratégicos para a Defesa Nacional, o nuclear de responsabilidade da Marinha e o espacial a cargo da Força Aérea Brasileira.

Com foco na estratégia da Defesa Cibernética o EB possui equipamentos modernos e pessoal capacitado para proteção da infraestrutura crítica do país.

Infraestruturas críticas são instalações, redes, sistemas, equipamentos físicos e de tecnologia da informação sobre os quais funcionam os serviços essenciais e cujo funcionamento é indispensável como saúde, segurança, bem-estar social, econômico e etc.

Muitas dessas estruturas estão conectadas entre as organizações e por isso tornam-se susceptíveis a ataques cibernéticos, capazes de gerar prejuízos de proporções devastadoras.

Pensando nisso torna-se fundamental a utilização de camadas de proteção complexas,

e adoção de estratégias para melhoria da segurança de equipamentos e sistemas de infraestrutura críticas da nação.

Umas das primeiras camadas de proteção seria o Firewall. Sendo empregado na primeira linha de defesa de um sistema ou rede contra ataques de intrusos por compor a primeira camada de segurança da informação, o Firewall se faz fundamental para a segurança de informações e dados sigilosos.

O Firewall em forma de hardware pode ser classificado como um sistema embarcado com função definida para a defesa.

Tendo tudo isso em vista, há uma crescente necessidade de se aprimorar a defesa cibernética de tais infraestruturas, e para isto o Firewall se faz uma das ferramentas de segurança da informação essenciais.

Através de uma revisão bibliográfica foi realizado um estudo com a finalidade de verificar tanto a importância de um sistema embarcado propriamente voltado para ciberdefesa, verificando suas vantagens e desvantagens em operatividade e aquisição, bem como alertar os gestores de Infraestruturas Críticas quanto a gravidade do assunto.

2 METODOLOGIA

Para elaboração desta revisão bibliográfica a busca para coleta de dados foi feita a partir de artigos atuais, livros texto, documentos sites da internet.Além da consulta em sites institucionais do próprio Exército Brasileiro. Foi feita uma busca ativa pelos termos “firewall”, “defesa cibernética”, “sistemas embarcados” e “infraestrutura crítica”, combinados com “no Exército Brasileiro” para contextualizar as pesquisas.

A partir da leitura dos títulos e resumos para seleção dos artigos mais adequados, foi realizada uma leitura minuciosa daqueles considerados fundamentais para a elaboração dos conceitos apresentados.

A partir de tais conceitos, buscamos compreender como estes poderiam ser extrapolados pela realidade atual, de forma prática, para Organizações que apresentam infraestruturas críticas, e por isso são considerados suscetíveis a ataques cibernéticos relevantes ao trabalho.

O presente estudo caracteriza-se por ser uma pesquisa do tipo aplicada, por ter como objetivo gerar conhecimento para aplicação prática para problemas específicos.A forma de abordagem utilizada foi a Qualitativa, pois é inviável a quantificação de tal abordagem em níveis Nacionais.

3 RESULTADOS E DISCUSSÃO

A revisão da literatura foi elaborada para permitir ao leitor tomar conhecimento de conceitos referentes ao presente trabalho, com abordagem de conceitos gerais de cibernética e textos específicos sobre o problema abordado na introdução.

3.1 MALWARE

3.1.1 CONCEITO DE MALWARE

Abreviação de “Software Malicioso”, Malware é um software projetado para fazer uma ação prejudicial, seja danificando arquivos, furtando dados sigilosos, ou até mesmo mantendo o dispositivo como “refém”. Malware é qualquer tipo de software criado para prejudicar ou explorar outro software ou hardware (REGAN e BELCIC, 2022). O malware é um software malicioso o qual é comum no meio cibernético. Para entendermos a necessidade de defesa cibernética, precisamos primeiro observar a vasta gama de softwares maliciosos, dos quais estamos expostos ao usufruir da tecnologia, bem como os prejuízos que eles podem implicar. O malware possui diversos tipos dos quais podemos distingui-los.

3.1.2 TIPOS DE MALWARE

Entre as diversas ameaças cibernéticas podemos elencar alguns tipos de malware utilizados atualmente.

3.1.2.1 VÍRUS

Vírus é um software malicioso que infecta arquivos limpos espalhando-se para os demais arquivos limpos. Não há controle após suas ações, ele danifica as funções de um sistema e exclui ou corrompe arquivos (REGAN e BELCIC, 2022). É um malware que se multiplica e corrompe os arquivos de um dispositivo.

3.1.2.2 CAVALO DE TRÓIA

Cavalo de Tróia é um malware que se disfarça como software autêntico, mas verdadeiramente possui um software malicioso. Sua função é entrar em um dispositivo dissimulando ter um conteúdo e após isso ele instalará outros malwares (REGAN e BELCIC, 2022).

3.1.2.3 SPYWARE

Spyware é um malware projetado, como o próprio nome indica, para espionagem. Ele se oculta em segundo plano e coleta dados do sistema, como senhas, localização GPS e informações financeiras (REGAN e BELCIC, 2022).

3.1.2.4 KEYLOGGER

Tipo de Spyware que se esconde no dispositivo para registrar a digitação do usuário. Memorizando quais as teclas o usuário com dispositivo infectado digita. Eles podem capturar por exemplo credenciais de login e números de cartão de crédito (REGAN e BELCIC, 2022).

3.1.2.5 SCREENLOGGER

Tipo de malware que permite armazenar a posição do cursor e a tela apresentada do monitor nos momentos em que o usuário executa um clique com o mouse ou a região que circunda o cursor do mouse quando ele é clicado. Muito utilizado para capturar senhas em teclados virtuais utilizados, por exemplo, em sites de internet banking (MIGLIANI, 2019).

3.1.2.6 RANSOMWARE

Ransomware é um malware que criptografa os arquivos de um dispositivo e ameaça apagar os dados caso não seja disponibilizado um resgate pela chave que descriptografa. Atualmente é uma das ameaças mais urgentes (REGAN e BELCIC, 2022). A tradução de “ransom” para o português é “resgate”. Como a própria palavra diz, o ransomware é um software de extorsão e frequentemente utilizado por hackers.

3.1.2.7 WORM

São malwares que diferem dos vírus por se espalharem em um arquivo hospedeiro. Tal software infecta redes inteiras de dispositivos, usando cada máquina infectada para infectar outras (REGAN e BELCIC, 2022).

3.2 VULNERABILIDADES E AMEAÇAS

3.2.1 VULNERABILIDADES CIBERNÉTICAS

Vulnerabilidade é uma fragilidade presente ou associada a ativos que manipulam ou processa informações, que ao ser explorada por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios de segurança da informação. Por si só não provoca incidentes, uma vez que se trata de elementos passivos, que necessitam de um ocasionador ou uma situação propícia que são as ameaças (SÊMOLA, 2003).

3.2.2 AMEAÇAS CIBERNÉTICAS

Ameaça é um agente ou potencial que causa incidentes e viola a segurança, por meio da exploração de vulnerabilidades, ou quando há uma circunstância, capacidade, ação favorável para isso. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade (SÊMOLA, 2003).

3.3. DEFESA CIBERNÉTICA E SEGURANÇA CIBERNÉTICA

3.3.1 DEFESA CIBERNÉTICA

Defesa Cibernética é conceituada no Glossário das Forças Armadas como conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente (BRASIL,2015,p. 85).

Logo a Defesa Cibernética é um conjunto de ações que irão providenciar proteção para os sistemas de informação.

3.3.2 SEGURANÇA CIBERNÉTICA

Refere-se à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da Administração Pública Federal ou APF (BRASIL, 2011,p. 18).

Outra definição para este conceito, por meio do Glossário das Forças Armadas é “Arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas” (BRASIL, 2015, p. 249).

Dessa forma, a segurança cibernética preocupa-se em reduzir ou eliminar vulnerabilidades da sociedade da informação do País e suas infraestruturas críticas da informação e em fazê-las voltar à condição de normalidade em caso de ataque, enquanto a defesa cibernética se preocupa em resguardar de ameaças (externas) e reagir, se for o caso, aos ataques ao “nosso” espaço cibernético (MANDARINO JUNIOR, 2011, p. 45)

A diferença essencial entre segurança cibernética e defesa cibernética é que enquanto aquela se preocupa em reduzir vulnerabilidades, esta se preocupa em resguardar de ameaças e reagir se necessário a ataques conforme especifica Mandarino Junior (2011, p.45).

3.3.3 FERRAMENTAS DE PROTEÇÃO CIBERNÉTICA

3.3.3.1 FIREWALL

Bloqueia softwares suspeitos. Será abordado no tópico 3.4 deste artigo.

3.3.3.2 SISTEMA DE DETECÇÃO DE INTRUSOS

Abreviado como IDS, o Sistema de Detecção de Intrusos trabalha de forma passiva, monitorando o tráfego da rede e alertando quanto a ataques e tentativas de invasão. Ele apenas detecta e alerta quanto ao intruso (SOFTWALL, 2018).

3.3.3.3 SISTEMA DE PREVENÇÃO DE INTRUSOS

Também chamado de IPS, o Sistema de Prevenção de Intrusos é capaz de identificar uma intrusão, analisar o quão perigosa ela é, enviar um alarme ao administrador e bloquear o intruso. Como software, o IPS previne e impede ciberataques (SOFTWALL, 2018).

3.3.3.4 CONTROLE DE ACESSO DE REDE

Conhecido como NAC, tem como propósito aumentar a proteção de uma rede de computadores corporativa. Dispositivos com fio ou sem fio podem ser monitorados e controlados pela ação do NAC (SIGMATELECOM, 2019)

3.3.3.5 ANTIVÍRUS

O software de proteção antivírus foi desenvolvido para prevenir, detectar e ajudar a remover ameaças de sistemas de computador. Essas ameaças assumem a forma de vírus de software e outros malwares, como ransomware, worms, cavalos de Tróia e adware (CISCO, 2022)

3.3.3.6 VPN

Uma rede virtual privada, ou VPN, é uma conexão criptografada de Internet do dispositivo para a rede. A conexão criptografada ajuda a garantir que dados confidenciais sejam transmitidos com segurança. Impede que pessoas não autorizadas acessem o tráfego e permite que o usuário realize um trabalho remoto. A tecnologia VPN é altamente usada em ambientes corporativos (CISCO, 2022).

3.3.3.7 BACKUP

Backup é uma cópia de segurança dos dados. Ela é armazenada em outro local, como uma nuvem ou dispositivo, por exemplo (CANALTECH, 2021).

3.4 FIREWALL

3.4.1 CONCEITO DE FIREWALL

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança. Os firewalls têm sido a linha de frente de defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a internet. Um firewall pode ser um hardware, software ou ambos (CISCO, 2022).

3.4.2 TIPOS DE FIREWALL

3.4.2.1 FIREWALL DE PROXY

Um firewall de proxy é um dos primeiros tipos de firewall e funciona como a passagem de uma rede para outra de uma aplicação específica. Servidores proxy podem oferecer recursos adicionais, como armazenamento em cache e segurança de conteúdo ao evitar conexões diretas e fora da rede. No entanto, isso também pode afetar a capacidade de taxa de transferência e as aplicações que eles podem comportar (CISCO, 2022).

3.4.2.2 FIREWALL COM INSPEÇÃO DE ESTADO

Atualmente conhecido como firewall tradicional, um firewall com inspeção de estado permite ou bloqueia tráfego de acordo com o estado, a porta e o protocolo. Ele monitora toda a atividade desde o momento em que uma conexão é aberta até que ela seja fechada. As decisões de filtragem são tomadas de acordo com as regras definidas pelo administrador e com o contexto, o que significa o uso de informações de conexões e pacotes anteriores que pertencem à mesma conexão (CISCO, 2022).

3.4.2.3 FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

Os firewalls evoluíram para além da simples filtragem de pacotes e inspeção estatística. A maioria das empresas está implantando firewall de próxima geração para bloquear ameaças modernas, como malware avançado e ataques na camada da aplicação.

De acordo com a definição do Gartner,Inc., um firewall de próxima geração deve incluir:

- Recursos padrão de firewall, como inspeção stateful;
- Prevenção de invasão integrada;
- Reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos;

Embora esses recursos estejam se popularizando entre as empresas, os NGFWs podem ser mais completos (CISCO, 2022).

3.4.2.4 NGFW FOCADO EM AMEAÇAS

Esses firewalls incluem todos os recursos de um NGFW tradicional e também

oferecem detecção e remediação avançadas de ameaças. Com um NGFW focado em ameaças, é possível:

● Saber quais recursos sofrem um risco maior com reconhecimento completo do contexto;

● Reduzir expressivamente o tempo entre a detecção e a limpeza com segurança retrospectiva que monitora continuamente atividades e comportamentos suspeitos mesmo após a inspeção inicial;

● Facilitar a administração e reduzir a complexidade com políticas unificadas que oferecem proteção durante todo o ciclo de ataque (CISCO,2022).

3.4.3 POSSIBILIDADES E LIMITAÇÕES

3.4.3.1 POSSIBILIDADES

Um firewall consegue realizar o controle de tráfego de dados, bloqueando possíveis ameaças de rede. Ele separa e filtra dados da rede local (LAN) face às redes externas (Wan) (CISCO, 2022).

O firewall em hardware é um método de proteção mais robusto que o firewall em software, podendo controlar um tráfego com maior número de dados com mais agilidade. Uma vez que o hardware funcionará apenas em função do firewall, o que cresce em muito o nível de controle que ele exercerá. Por mais que seus gastos como a sua compra, manutenção e implementação sejam superiores às da versão em software, os gastos que podem ocorrer por parte de uma invasão a uma infraestrutura crítica provavelmente serão superiores (STORAGEONE,2021). É importante que os gestores de Infraestruturas Críticas investem em segurança da informação. Analogamente a um seguro, o firewall em hardware serve para evitar um prejuízo maior.

3.4.3.2 LIMITAÇÕES

Firewalls são componentes cruciais na segurança de uma rede. Porém, eles não são completamente perfeitos. Para que seu funcionamento seja pleno, é necessário que todo o fluxo de dados passe pelo firewall. Por isso, diversos problemas não podem ser resolvidos através do uso de um firewall. Vejamos alguns deles:

● Um firewall não consegue impedir um ataque cuja origem e destino seja a rede interna, pois os dados não passarão por ele, tornando-o ineficaz nesse tipo de ataque;

● Os firewalls não aumentam a força de senhas e nem previnem o uso inadequado das mesmas. Da mesma forma, eles são ineficazes em ataques não-técnicos como Engenharia Social;

● Firewalls não conseguem impedir que usuários acessem sites com códigos maliciosos, tornando necessária a conscientização dos usuários neste sentido (UFRJ, 2022).

3.5 INFRAESTRUTURAS CRÍTICAS

3.5.1 CONCEITO

Infraestruturas Críticas são instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2014, p.19). Podemos citar como exemplos de Infraestruturas Críticas os setores de energia, telecomunicações, financeiro, transporte, distribuição de água, saúde, petroquímica e petróleo, dentre diversos outros.

FIGURA 1

Fonte: adaptado de GP3/CAEM (2018).

3.6 ATAQUES CIBERNÉTICOS

3.6.1 CONCEITO

Um ataque cibernético é uma tentativa de desabilitar computadores, roubar dados ou usar um sistema de computador violado para lançar ataques adicionais. Os criminosos virtuais usam diferentes métodos para lançar um ataque cibernético que incluem malware, phishing, ataque man-in-the-middle ou outros métodos (UNISYS, 2022).

3.6.2 FINALIDADE

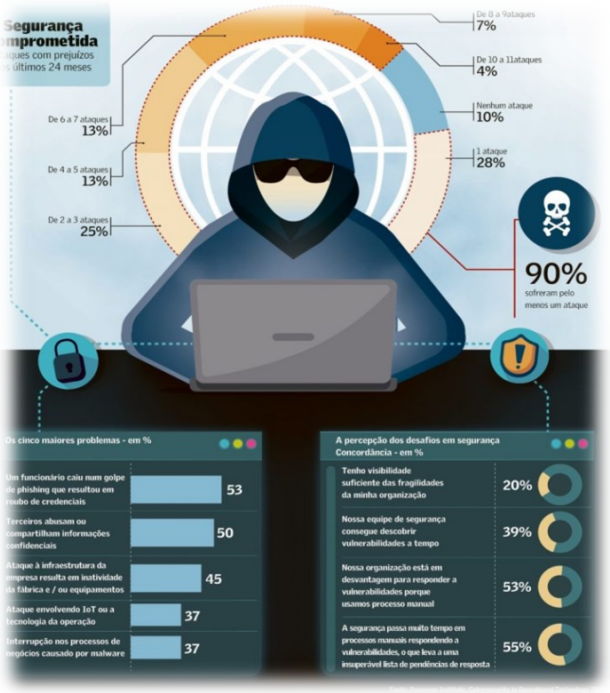
A finalidade de um ataque cibernético por meio de um atacante, chamado de Hacker, é, em sua grande maioria interromper, desativar, destruir ou controlar de maneira má intencionada uma infraestrutura de computação. Os hackers tem algumas formas para obter sucesso em seus ataques, como por meio de softwares mal intencionados que violam as vulnerabilidades, por meio de links fraudulentos que objetivam roubar ou obter dados confidenciais das vítimas ou por meio de ataques de espionagem em que o hacker se insere em uma transação entre duas vítimas.

3.6.3 ATAQUES RECENTES

Recentemente tem sido dada uma importante atenção aos ataques cibernéticos, haja vista os “estragos” que os mesmos podem causar em grandes empresas, em infraestruturas consideradas críticas e até mesmo governos.Um fato que confirma isso é o notável e recente aumento,por parte das empresas brasileiras, das buscas pelos chamados seguros cibernéticos. A Confederação Nacional das Seguradoras (CNseg) divulgou uma pesquisa no dia 26/05/2022 em que diz que tal procura cresceu 41,5% no primeiro trimestre deste ano, quando comparado ao ano anterior. “Ainda teremos um crescimento grande no setor. Os ataques cibernéticos têm sido cada vez mais frequentes e a proteção oferecida pelo seguro é uma tranquilidade a mais para as empresas evitarem maiores prejuízos.” Afirmou Dyogo Oliveira, presidente da CNseg.

Um ponto importante a ser explorado é o fato das empresas, estabelecimentos comerciais, o comércio em geral terem praticamente reduzido a zero os atendimentos presenciais devido à pandemia do COVID-19, assim sendo, a maioria “migrou” para suas vendas para o meio digital.Os empresários do E-commerce, como é chamada essa modalidade, viram a necessidade de buscar uma proteção para seus negócios.

FIGURA 2



Fonte: SOPESP (2019).

4. CONCLUSÃO

O objeto do nosso estudo foi verificar a eficácia que um firewall, como sistema embarcado, poderia exercer em Infraestruturas Críticas. Para este objetivo foi realizada uma revisão literária para identificarmos alguns conceitos basilares inerentes ao assunto. Após a explanação dos conceitos que envolvem a defesa cibernética face às Infraestruturas Críticas, foram analisadas tanto as vantagens quanto às desvantagens em se obter um firewall em hardware. Foi tirado como conclusão que o firewall em hardware possui maior capacidade de proteção para empresas de médio e grande porte, e que são mais custosos que o firewall em software.

Foi observado,também que as Infraestruturas Críticas se tornaram alvo frequente de hackers na era da tecnologia em

que vivemos por meio de ataques cibernéticos. A pesquisa do presente artigo analisou que é interessante que os gestores de tais organizações adquiram um firewall em hardware, os quais apesar de serem mais custosos em termos de compra, manutenção e implementação, fornecem maior segurança que o firewall em software e previnem um gasto ainda maior. As informações sigilosas ou mesmo os serviços de uma infraestrutura crítica ao serem comprometidos, além de gerar um prejuízo exacerbado, podem comprometer vidas, como por exemplo ataques recentes a base de dados de um hospital.

A pandemia trouxe essa necessidade à tona na medida em que as empresas aderiram, em massa, à digitalização de seus negócios. Os custos para manutenção da segurança cibernética são elevados, porém mais vale investir em seguros do que perder elevadas quantias de dinheiro para os hackers que se atualizam cada vez mais. Um exemplo é o recente ataque ao famoso Grupo de NFT (Not Fungible Token) Bored Ape Yatch Club que teve sua conta violada e os possuidores de tais NFT's perderam milhões de dólares em uma única ação dos cibercriminosos.

A intenção deste artigo foi demonstrar, por meio da revisão de alguns assuntos inerentes à defesa cibernética, que existem artifícios espalhados pela rede e, ainda pior, pessoas mal intencionadas e que desejam adquirir benefícios de forma ilícita. Através de alguns exemplos dados no decorrer deste trabalho, podemos tirar por conclusão que vale a pena, sim, investir nos firewalls de hardware para que as infraestruturas críticas, principalmente as ligadas à defesa nacional, estejam cada vez mais seguras frente às ameaças reais que assolam o espaço cibernético Brasileiro.

5. REFERÊNCIAS

BAITZ SOLUTIONS Ciberataques em empresas de saúde e hospitais aumentaram durante a pandemia do COVID-19<https://baitzsolutions.com.br/blog/2020/06/25/ciberataques-em-empresas-de-saude-e-hospitais-aumentaram-durante-a-pandemia-do-covid-19/> Acesso em 17/03/2022.

BARROS, O. S. R; GOMES, U. M. Desafios Estratégicos para a Segurança e Defesa Cibernética. Brasília: Secretaria de Assuntos Estratégicos, 2011, p. 204.

BRASIL, Ministério da Defesa. MD31-M-07: doutrina militar de defesa cibernética. Brasília: EMCFA, 2014.

BRASIL, Ministério da Defesa. MD35-G-01: Glossário das Forças Armadas. 5 Ed.Brasília: EMCFA, 2015.

CANALTECH, O que é Backup e por que ele é importante?<https://canaltech.com.br/software/o-que-e-backup-e-por-que-ele-e-importante/> Acesso em 20/05/2022.

CISCO. O que é um firewall. <https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html> Acesso em 17/03/2022.

FACULDADE UNYLEYA. Afinal, o que é defesa cibernética. <https://blog.unyleya.edu.br/bibyte/curso-de-defesa-cibernetica/#:~:text=A%20defesa%20cibern%C3%A9tica%20se%20refere,que%20atuam%20no%20mundo%20virtual> Acesso em 17/03/2022.

MIGLIANI.Felipe.Conheça os 4 principais tipos de 'spyware' e mantenha seu dispositivo protegido.<https://observatoriodacomunicacao.org.br/artigos/conheca-os-4-principais-tipos-de-spyware-e-mantenha-seu-dispositivo-protegido-por-felipe-migliani/> Acesso em 20/05/2022.

HORNO, José Mateo del. Infraestruturas Críticas e Cibersegurança. <http://ingenieriaseguridad.telefonica.com/not%C3%ADcia/2016/11/07/Infraestruturas-Cr%C3%ADticas-e-Ciberseguran%C3%A7a.html> Acesso em 17/03/2022.

JOSEPH REGAN E IVAN BELCIC, O que é

malware? O Guia Definitivo para Malware. <https://www.avg.com/pt/signal/what-is-malware>Acesso em 20/05/2022.

JUNIOR, Raphael Mandarino. Tendências Globais em Segurança e Defesa Cibernética: Segurança e Defesa Cibernética. In: Desafios Estratégicos para a Segurança e Defesa Cibernética. Brasília: [s. n.], 2011. p. 45.

MARKETING WTSNET. Melhores práticas de firewall para bloquear ataques ransoware.<https://www.wtsnet.com.br/segurança/melhores-praticas-firewall-ataques-ransomware/> Acesso em 17/03/2022.

SANTOS, Yasser O que é um firewall e quais suas funções <https://tripla.com.br/o-que-e-um-firewall/>. Acesso em 17/03/2022.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva da segurança da informação. 9º Reimpressão. Rio de Janeiro: Elsievier, 2003 UFRJ. FIREWALLS<HTTPS://WWW.GTA.UFRJ.BR/GRAD/15_1/FIREWALL/LIMITACOESDOFIREWALL.HTML> Acesso em 20/05/2022.

SIGMA TELECOM, NAC Network Access Control: Entenda o que é <https://www.sigmatelecom.com.br/o-que-e-network-access-control/> Acesso em 20/05/2022.

SOFTWALL. Firewall, IPS, IDS e WAF: como cada um atua? <https://www.softwall.com.br/blog/firewall-ips-ids-e-waf-como-cada-um-atua/>Acesso em 20/05/2022.

STORAGEONE, Firewall de hardware x firewall de software: Entenda as diferenças e o mais adequado para sua empresa.<https://www.sto1.com.br/blog/seguranca-de-dados/firewall-de-hardware-ou-software/> Acesso em 21/05/2022.

UNISYS, Securing Your Tomorrow.https://www.unisys.com/pt/glossary/cyber-attack/, Acessado em 17/05/2022

WILLIAN, Fonseca. O que são bots e botnets? <HTTPS://WWW.TECMUNDO.COM.BR/SPYWARE/2330-O-QUE-SAO-BOTS-E-BOTNETS-.HTM> Acesso em 20/05/2022.