Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.23, n.1, p.13-31, 2023.
DOI: 10.18762/1982-4920.20230002

ANÁLISE DE VULNERABILIDADES E AMEAÇAS EM SERVIDORES ON-PREMISES: ESTRATÉGIAS DE PREVENÇÃO A INCIDENTES

Paulo César dos Santos Junior, André Castro Rizo.

RESUMO

Este artigo apresenta uma análise das vulnerabilidades e ameaças em servidores on-premises, destacando a importância de estratégias de prevenção e resposta a incidentes. A crescente adoção de tecnologias digitais tem levado a um aumento significativo das ameaças cibernéticas, tornando a segurança dos servidores on-premises uma preocupação constante para as empresas. Neste sentido, o estudo tem como objetivo analisar as principais vulnerabilidades e ameaças em servidores on-premises, bem como estratégias eficazes para prevenção e resposta a incidentes. A metodologia consiste em uma pesquisa sistemática da literatura especializada e pesquisa bibliográficas. Os resultados indicam que as principais vulnerabilidades em servidores on-premises estão relacionadas à falta de atualização de software, senhas fracas e acesso não autorizado. As estratégias de prevenção incluem a implementação de atualizações de software regulares, uso de senhas fortes e autenticação em dois fatores, além de controles de acesso efetivos. Para a resposta a incidentes, é recomendado o desenvolvimento de planos de contingência e a realização de treinamentos regulares para a equipe de segurança da informação. Conclui-se que a análise de vulnerabilidades e ameaças em servidores on-premises é essencial para garantir a segurança das informações e dados das empresas, e a adoção de estratégias de prevenção e resposta a incidentes pode minimizar os riscos de violações de segurança.

Palavras-chave: Servidores on-premises; Segurança da informação; Análise de vulnerabilidades; Prevenção de incidentes; Estratégias de segurança.

Abstract

This article presents an analysis of vulnerabilities and threats in on-premises servers, highlighting the importance of prevention strategies and incident response. The growing adoption of digital technologies has led to a significant increase in cyber threats, making the security of on-premises servers an ongoing concern for organizations. In this context, the study aims to analyze the main vulnerabilities and threats in on-premises servers, as well as effective strategies for prevention and incident response. The methodology consists of a systematic review of specialized literature and bibliographic research. The results indicate that the primary vulnerabilities in on-premises servers are related to software update deficiencies, weak passwords, and unauthorized access. Prevention strategies include the implementation of regular software updates, the use of strong passwords and two-factor authentication, as well as effective access controls. For incident response, the development of contingency

plans and the conduction of regular training for the information security team are recommended. It is concluded that the analysis of vulnerabilities and threats in on-premises servers is essential for ensuring the security of organizational information and data, and the adoption of prevention strategies and incident response can mitigate the risks of security breaches.

Keywords: On-premises servers; Information security; Vulnerability analysis; Incident prevention; Security strategies.

1 INTRODUÇÃO

A segurança da informação é um tema cada vez mais relevante no cotidiano das pessoas em todo o mundo, e no Brasil, desde a publicação da Lei Geral de Proteção de Dados (LGPD) em 2018, as discussões sobre o assunto estão cada vez mais em evidência. A segurança da informação em conjunto com a LGPD e as normas da família ISO 27000 (normas técnicas voltadas para padronização e boas práticas relacionadas à segurança da informação) abrangem os aspectos das informações, incluindo sua classificação e tratamento adequado.

Em ambientes corporativos, a segurança da informação se tornou uma preocupação cada vez mais relevante, especialmente com a crescente adoção de tecnologias digitais e a ampliação do uso de servidores on-premises. Com o armazenamento de dados sensíveis em servidores locais, a proteção contra ameaças cibernéticas e vulnerabilidades se torna uma questão crítica para a continuidade dos negócios e a manutenção da confiança dos clientes.

Neste contexto, o presente estudo tem como objetivo analisar as vulnerabilidades e ameaças em servidores on-premises, identificar as principais estratégias de prevenção e resposta a incidentes, e discutir as implicações desses fatores para a segurança da informação em ambientes corporativos. A adoção de estratégias de prevenção e resposta a incidentes é essencial para garantir a integridade dos dados e informações, bem como para minimizar os riscos de violações de segurança.

Em suma, este estudo visa contribuir para o desenvolvimento de estratégias de segurança da informação mais eficazes em ambientes corporativos, proporcionando uma melhor compreensão dos principais desafios e soluções relacionados à segurança de servidores on-premises.

2 REFERENCIAL TEÓRICO

O objetivo deste estudo consiste na análise de estudos e pesquisas que tratam das vulnerabilidades e ameaças em servidores on-premises, bem como estratégias de prevenção e resposta a incidentes.

Um servidor on-premises é um sistema de computador físico operado e mantido dentro das instalações de uma organização. Ao contrário dos servidores em nuvem, que são gerenciados remotamente por provedores de serviços, um servidor on-premises é controlado internamente pela própria organização.

Ele é utilizado para armazenar, processar e fornecer serviços e recursos de rede, como armazenamento de dados, hospedagem de aplicativos e compartilhamento de arquivos.

Ter um servidor on-premises proporciona à organização controle direto sobre sua infraestrutura de TI, mas também acarreta responsabilidades adicionais, como a manutenção de hardware e software, segurança e backup dos dados.

A seguir, serão apresentados os principais resultados encontrados na literatura especializada.

2.1 Vulnerabilidades em servidores on-premises

A falta de atualização de software, senhas fracas e acesso não autorizado são algumas das principais vulnerabilidades encontradas em servidores on-premises. Segundo Joy LePree (Security Magazine, 2023), entre 2021 e 2022 houve o aumento médio de 38% de ataques cibernéticos em todo o globo, só no Reino Unido o aumento foi de 77%, tais números são bem expressivos se considerarmos que o setor mais afetado nesse período foi o de saúde pública.

No Brasil, em 2022, segundo relatório da empresa Sophos, atualmente uma das líderes no mercado de cibersegurança, 68% das empresas que possuem suas sedes estabelecidas no país foram alvo de ataques cibernéticos (Infomoney, 2023).

Muitas pessoas desconhecem os riscos da utilização de senhas fracas e a falta de autenticação em dois fatores, e por isso também são apontadas como fatores

críticos para a segurança de servidores on-premises, permitindo a fácil invasão de hackers e violações de segurança (Security Report, 2022).

Além disso, a falta de controle de acesso e a má configuração dos servidores são outras vulnerabilidades comuns em ambientes corporativos. Muitas vezes, os servidores possuem serviços mal configurados ou desatualizados, o que abre brechas para a exploração de vulnerabilidades conhecidas, geralmente catalogadas em bases de dados como a CVE - *Common Vulnerabilities and Exposures* (Vulnerabilidades e Exposições Comuns).

2.2 Implicações para a segurança da informação em ambientes corporativos

As vulnerabilidades e ameaças em servidores on-premises apresentam implicações significativas para a segurança da informação em ambientes corporativos. A violação da segurança dos servidores pode resultar em perda de dados, interrupção dos serviços e danos à reputação da empresa.

Além disso, a não conformidade com leis e regulamentos de segurança pode resultar em penalidades financeiras e jurídicas. Nesse sentido, a adoção de medidas eficazes de prevenção e resposta a incidentes é essencial para garantir a segurança da informação em ambientes corporativos.

2.3 Tecnologias emergentes para a segurança de servidores on-premises

Com a evolução das tecnologias, novas soluções de segurança têm surgido para proteger os servidores on-premises. Uma delas é o uso de inteligência artificial e aprendizado de máquina para detectar ameaças em tempo real e automatizar a resposta a incidentes (ZEQUIM; RIBEIRO, 2022). Além disso, tecnologias como blockchain entre outras também têm sido exploradas para aumentar a segurança em servidores on-premises.

2.4 Desafios e tendências futuras na segurança de servidores on-premises

Apesar das diversas estratégias e tecnologias existentes para aumentar a segurança em servidores on-premises, ainda existem desafios a serem enfrentados

nessa área. Um deles é a necessidade de equilibrar a segurança com a facilidade de uso e acessibilidade, de forma a não comprometer a produtividade dos usuários.

Além disso, o aumento do número de dispositivos conectados à rede corporativa, como dispositivos IoT, pode representar novas vulnerabilidades para os servidores on-premises (OLIVEIRA et al, 2019).

Uma tendência futura na segurança de servidores on-premises é o uso crescente de soluções de segurança baseadas em nuvem, que podem oferecer recursos avançados de prevenção e detecção de ameaças, além de permitir a gestão centralizada de múltiplos servidores (GALEGO; DUARTE; MARTINHO, 2022).

Outra tendência é o uso de soluções de segurança integradas, que combinam diferentes tecnologias e estratégias para fornecer uma proteção mais abrangente aos servidores on-premises (FREITAS, 2011).

2.5 Importância da segurança de servidores on-premises na era da transformação digital

Com a crescente digitalização das empresas e a adoção de tecnologias como cloud computing, big data e IoT, a segurança de servidores on-premises se torna ainda mais importante. Isso porque esses servidores geralmente contêm informações críticas e sensíveis, como dados de clientes e propriedade intelectual, que podem ser alvo de ataques cibernéticos sofisticados.

Além disso, a conformidade com regulamentações como a LGPD no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) na Europa torna ainda mais crucial a adoção de medidas de segurança eficazes em servidores on-premises, para garantir a proteção dos dados dos clientes e evitar penalidades por não conformidade.

Nesse sentido, é fundamental que as empresas se mantenham atualizadas sobre as melhores práticas e tecnologias de segurança para servidores on-premises, a fim de garantir a integridade, confidencialidade e disponibilidade de seus dados e sistemas.

2.6 A importância do monitoramento de vulnerabilidades e ameaças em servidores on-premises

Uma das principais estratégias para garantir a segurança de servidores on-premises é o monitoramento constante de vulnerabilidades e ameaças. Isso envolve a realização de testes regulares de penetração, análise de logs e eventos de segurança, e o uso de ferramentas de detecção de ameaças avançadas.

O monitoramento de vulnerabilidades e ameaças permite que as empresas identifiquem proativamente possíveis pontos fracos em seus sistemas e tomem medidas preventivas para evitar ataques cibernéticos. Além disso, em caso de incidentes de segurança, o monitoramento pode ajudar a detectar rapidamente a origem do ataque e minimizar os danos causados.

3 ESTRATÉGIAS E FERRAMENTAS DE PREVENÇÃO E MITIGAÇÃO DE INCIDENTES

A adoção de ferramentas de monitoramento e detecção de ameaças também é apontada como uma estratégia eficaz para a prevenção e resposta a incidentes em servidores on-premises (VALE, 2017).

Além do monitoramento constante, existem diversas estratégias de prevenção e resposta a incidentes que as empresas podem adotar para aumentar a segurança em seus servidores on-premises. Uma dessas estratégias é a implementação de políticas de segurança claras e abrangentes, que incluam procedimentos de autenticação e autorização de usuários, restrições de acesso a recursos críticos e monitoramento de atividades suspeitas (SANTOS; SOARES; GIRALDI, 2018).

Outra estratégia é a utilização de soluções de segurança avançadas, como firewalls, antivírus e soluções de prevenção de intrusão. Essas soluções podem ajudar a proteger os servidores on-premises contra diferentes tipos de ataques, incluindo malware, phishing e ataques de negação de serviço.

Por fim, é fundamental que as empresas estabeleçam planos de contingência e recuperação em caso de incidentes de segurança. Isso inclui a definição de procedimentos claros de notificação e resposta a incidentes, bem como a realização de backups regulares dos dados do servidor para garantir a recuperação rápida em caso de perda de dados.

Para prevenir e responder a incidentes de segurança em servidores on-premises, a literatura especializada destaca a importância de se implementar medidas como atualizações de software regulares, uso de senhas fortes e autenticação em dois fatores, além de controles de acesso efetivos (WANGENHEIM et al, 2016).

Além disso, a realização de treinamentos regulares para a equipe de segurança da informação e o desenvolvimento de planos de contingência são outras estratégias importantes para a prevenção e resposta a incidentes em servidores on-premises (HINTZBERGEN et al, 2018).

Todas essas diretrizes devem ser bem definidas e estipuladas em uma Políticas de Segurança da Informação (PSI), sendo que esta deve ser do conhecimento de todos os envolvidos nos processos quando aplicada em uma organização.

Além das estratégias mencionadas anteriormente, existem outras medidas que podem ser adotadas para aumentar a segurança em servidores on-premises. Uma delas é a implementação de firewalls de próxima geração, que oferecem recursos de prevenção e detecção de ameaças mais avançados em comparação aos firewalls tradicionais.

Conforme Felipe, Leonardo e Rodrigo descrevem, o

> Firewall é uma solução de segurança baseada em hardware ou software, que a partir de um conjunto de regras ou instruções, analisa o trafego da rede para diferenciar operações válidas ou inválidas dentro de uma rede corporativa. Um firewall analisa o tráfego de rede entre a internet e a rede privada ou entre redes privadas. (NEVES; MACHADO; CENTENARO, 2019, p. 11).

Com base nas definições anteriormente citadas, podemos concluir que um firewall vai além de uma ferramenta de bloqueio e desempenha um papel importante na gestão de redes de computadores. A maioria das soluções disponíveis no mercado oferece diversas funções e complementos, incluindo IPS, IDS, Proxy e WebFilters.

IPS/IDS (Sistema de Prevenção de Intrusão e Sistema de Detecção de Intrusão) são essenciais em uma infraestrutura de rede, pois analisam os pacotes de dados trafegados na rede e os comparam com um banco de dados de ameaças cibernéticas, que contém assinaturas conhecidas. Um IDS é um sistema de monitoramento, enquanto um IPS é responsável pelo controle de intrusões. Juntos, eles impedem o tráfego de pacotes não legítimos na rede.

Um servidor proxy oferece várias soluções, sendo as mais conhecidas o serviço de mediação e bloqueio de conteúdo. Como mediador, o servidor proxy recebe as

requisições de conexões de uma determinada rede e as encaminha para a Internet. Seu uso oferece várias vantagens, como a capacidade de analisar e armazenar as requisições.

Ao analisar uma requisição, o servidor proxy pode validar seu conteúdo e determinar se é prejudicial ou não para a rede. As requisições mais frequentes são armazenadas em cache, reduzindo o consumo de banda larga.

O filtro ou bloqueador de conteúdo é outra função comumente utilizada, permitindo ao administrador da rede criar regras para bloquear acesso a tipos específicos de conteúdo ou sites, como redes sociais, violência e pornografia.

Embora o uso de um servidor proxy seja fundamental em uma infraestrutura de rede, algumas organizações optam por não o adotar devido à possível lentidão no acesso à Internet, especialmente quando há muitas solicitações simultâneas, o que pode frustrar os usuários. Além disso, com o aumento dos serviços e links de banda larga, o uso de cache se torna cada vez menos necessário.

O WebFilter, ou filtro de conteúdo, é um tipo de serviço que pode ser implementado por soluções autônomas sem a necessidade de servidores proxy. Esses filtros possuem funções semelhantes aos bloqueadores ou filtros de conteúdo de um servidor proxy.

Eles desempenham um papel fundamental na segurança da informação nas infraestruturas de redes de computadores. Seu funcionamento básico requer apenas a configuração de listas brancas (sites permitidos) e listas negras (sites bloqueados), que geralmente já vêm pré-configuradas nas soluções de mercado.

O bloqueador de conteúdo é outra função do WebFilter, permitindo o bloqueio de conteúdo por categoria, como violência ou pornografia. No entanto, o bloqueador de conteúdo requer maior capacidade computacional, pois compara o conteúdo com uma base de dados conhecida, o que pode resultar em lentidão no acesso.

Normalmente, os administradores de infraestruturas de redes optam pelo uso de bloqueios e filtros de sites, pois exigem menos capacidade computacional e, consequentemente, causam menor lentidão no acesso à Internet.

Outra estratégia importante é a segmentação da rede, que consiste em dividir a rede em segmentos menores e protegidos por firewalls, dificultando a propagação de ameaças em toda a rede corporativa. Além disso, a criptografia dos dados em trânsito

e em repouso pode fornecer uma camada adicional de segurança aos servidores on-premises.

No conceito de Segurança da Informação em infraestrutura de redes e servidores On-premise, é de extrema importância o uso de backup em suas aplicações. O backup, também conhecido como cópia de segurança, consiste na criação de cópias dos dados específicos com o objetivo de restaurá-los no caso de perda dos originais (FARIA, 2010).

Basicamente, um servidor ou serviço de backup tem como função principal manter a integridade das cópias de segurança dos dados armazenados nele. Por esse motivo, é crucial que sejam confiáveis e robustos.

Devido à grande quantidade de dados que trafegam e são armazenados nos backups, essas soluções precisam estar em conformidade com diversos aspectos de segurança, sendo os pilares da segurança o principal foco das organizações que oferecem esse tipo de serviço.

Nos casos em que a própria organização mantém esse tipo de serviço, é necessário adotar uma abordagem mais rigorosa, uma vez que a falha em qualquer processo interno pode resultar em perdas irreversíveis.

Duas soluções amplamente utilizadas no mercado são o Veeam e o Bacula. Ambas possuem o mesmo propósito e contam com uma ampla comunidade de especialistas.

Tanto o Veeam quanto o Bacula são gerenciadores de backup, onde o funcionamento é baseado na comunicação entre o agente (software) instalado no terminal que necessita do serviço de backup e o servidor, que contém as regras e políticas de backup.

Uma prática recomendada é estabelecer políticas sólidas para manter os serviços de backup. Além disso, é importante utilizar criptografia nas comunicações entre o servidor e os agentes, a fim de evitar a captura de dados durante as transferências.

Um aspecto importante a ser destacado é a realização de testes nos backups gerados, a fim de verificar a legibilidade e a usabilidade deles. Esses testes devem ser validados por meio de um Plano de Continuidade de Negócio (PCN).

Existem outros aspectos técnicos a serem observados para garantir a segurança do ambiente, porém, o fator humano é primordial e influencia diretamente em todos os outros elementos abordados neste trabalho.

Atualmente, é indiscutível a presença do aspecto humano nas organizações, sendo implícito que se deve dar atenção a esse aspecto, uma vez que "este elemento traz riscos à segurança da informação, uma vez que pessoas podem obter acesso legítimo a informações, conhecem a organização e sabem a localização de ativos valiosos" (CARNEIRO; ALMEIDA, 2013).

Com base no assunto abordado anteriormente, pode-se afirmar que as pessoas envolvidas nos processos de uma organização que utiliza tecnologia da informação podem representar riscos aos ativos de infraestrutura de rede e servidores on-premise.

Devido à existência de vários cenários nos quais as pessoas podem estar envolvidas, os diretores e gestores de TI devem buscar maneiras de minimizar possíveis interferências humanas na infraestrutura e nos servidores.

Nesses casos, muitas organizações começam a implementar suas próprias Políticas de Segurança da Informação, nas quais descrevem e documentam informações e suas respectivas tratativas.

A PSI deve abordar a classificação dos dados e recursos de informação, além de tratar das regras e padrões para a proteção dos dados. Com isso, busca-se manter os pilares da Segurança da Informação, como confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

A implementação da PSI deve ser acompanhada de documentação que contenha procedimentos, regras e padronizações estipuladas. Essa documentação também deve abordar informações sobre os indicadores que serão utilizados para avaliar o desempenho da PSI na organização, além de tratar da conscientização e treinamento dos envolvidos.

É fundamental que uma PSI aborde as políticas de acesso aos ativos de TI, sejam eles acessos lógicos ou físicos. O controle dos acessos deve ser realizado de forma minuciosa, com o cadastro de todos os usuários e registros de acesso e permanência. É importante ressaltar que as contas de usuários devem ser únicas e intransferíveis.

No caso dos acessos lógicos, as organizações devem estabelecer políticas sobre a criação e uso de senhas pelos usuários, orientando-os sobre a importância de senhas fortes e como criá-las e mantê-las de forma segura. Para isso, podem ser utilizadas soluções seguras e reconhecidas no mercado, como o KeePass e o NordPass, que auxiliam na gestão de senhas.

Em resumo, a análise da literatura aponta para a importância de se implementar medidas eficazes de prevenção e resposta a incidentes em servidores on-premises, dada a crescente sofisticação das ameaças cibernéticas.

As vulnerabilidades mais comuns em servidores on-premises incluem a falta de atualização de software, senhas fracas e acesso não autorizado, e estratégias como atualizações regulares, uso de senhas fortes, controles de acesso efetivos, monitoramento e detecção de ameaças, além de treinamento e desenvolvimento de planos de contingência, podem ajudar a mitigar essas vulnerabilidades.

Além disso, tecnologias emergentes como inteligência artificial, blockchain e edge computing têm potencial para fornecer soluções mais avançadas de segurança para servidores on-premises.

4 METODOLOGIA

A pesquisa bibliográfica foi realizada por meio de uma revisão sistemática da literatura em revistas científicas especializadas em segurança da informação. Foram selecionados artigos científicos que abordam o tema de análise de vulnerabilidades e ameaças em servidores on-premises.

Para a seleção dos artigos, foram utilizados os seguintes critérios:

Estudos que apresentam análises de vulnerabilidades e ameaças em servidores on-premises;

Estudos que apresentam estratégias de prevenção e resposta a incidentes relacionados a servidores on-premises;

Artigos publicados em revistas científicas ou de alto impacto na área de segurança da informação.

A revisão sistemática da literatura foi realizada em duas etapas:

Busca: Foram realizadas buscas nas seguintes bases de dados: Google Acadêmico e sites que abordam sobre o tema de tecnologia da informação, sendo esses brasileiros e internacionais.

As palavras chaves utilizadas foram: "servidores on-premises", "analise de vulnerabilidades", "segurança da informação", "tecnologias emergentes", "política de segurança da informação".

Seleção dos artigos: Após a busca, os artigos foram selecionados com base nos critérios estabelecidos e analisados quanto a relevância para a pesquisa.

A análise dos artigos selecionados foi realizada por meio de uma leitura crítica e sistemática. Foram identificadas as principais vulnerabilidades e ameaças em servidores on-premises, bem como as estratégias mais eficazes de prevenção e resposta a incidentes.

Por fim, foram apresentados os resultados da pesquisa em forma de artigo científico, incluindo uma revisão da literatura, análise dos artigos selecionados e discussão dos principais resultados encontrados.

5 RESULTADOS E DISCUSSÃO

A análise sistemática da literatura permitiu identificar as principais vulnerabilidades e ameaças em servidores on-premises, bem como as estratégias mais eficazes de prevenção e resposta a incidentes.

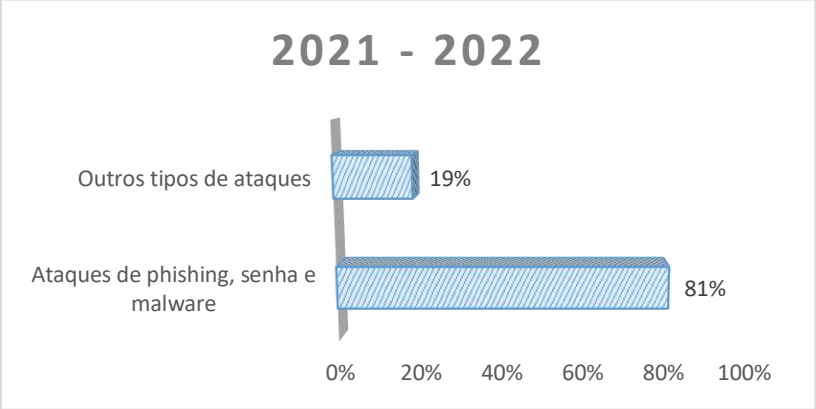
Dentre as vulnerabilidades mais comuns identificadas nos artigos selecionados, destacam-se: a falta de atualização dos sistemas operacionais e softwares instalados, a falta de configurações adequadas de segurança, a falta de políticas de senhas fortes e a falta de monitoramento adequado do tráfego de rede.

Com relação às ameaças, os artigos apontaram as seguintes: malware, ataques de força bruta, ataques de negação de serviço (DoS), ataques de phishing, ataques de engenharia social e ações maliciosas de pessoas que estão dentro das organizações (insiders).

De acordo com o relatório da Fortinet, o número de ataques em organizações aumentou em 53% em 2022 em comparação com o ano anterior. As organizações relataram enfrentar cinco ou mais tentativas de violação de segurança.

O relatório também revelou que 81% dos ataques ocorridos entre 2021 e 2022 estavam relacionados a phishing, senhas e malwares. Os 19% restantes foram atribuídos a outros métodos de ciberataque.

Gráfico 1 – Tipos de ciberataques entre os anos de 2021 e 2022 no mundo.

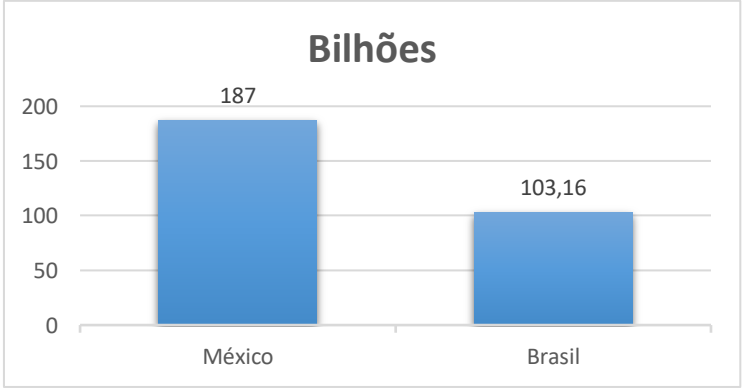


Fonte: Fortinet.

Com base nos dados mencionados, o relatório da Fortinet destaca que os gestores das organizações estão aumentando a demanda por profissionais especializados em segurança da informação. Esses profissionais desempenham um papel crucial na implementação de políticas mais robustas e na mitigação de vulnerabilidades. Essa tendência reforça as indicações e preocupações abordadas neste artigo.

Outro aspecto relevante a ser destacado é o expressivo aumento de 16% nas tentativas de ciberataques no Brasil entre os anos de 2021 e 2022. Os números saltaram de 88,5 bilhões para 103,16 bilhões, colocando o Brasil como o segundo país com maior incidência de ciberataques na América Latina.

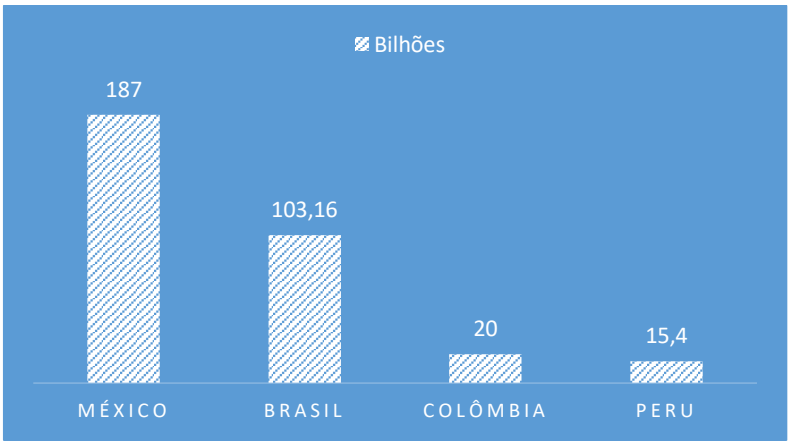
Gráfico 2 – Quantidade de tentativas de ataques cibernéticos no Brasil.



Fonte: FEBRABAN.

Esses dados revelam que o país fica atrás apenas do México, que registrou 187 bilhões de tentativas, e supera a Colômbia e o Peru, com 20 bilhões e 15,4 bilhões respectivamente. Essas informações são baseadas em dados fornecidos pela FEBRABAN (Federação Brasileira de Bancos).

Gráfico 3 – Países com maior quantidade de tentativas de ataques cibernéticos na América Latina.



Fonte: FEBRABAN.

Com base nos dados apresentados, fica evidente a importância de abordar a segurança da informação em servidores on-premises de forma cuidadosa e diligente. A fim de mitigar vulnerabilidades e proteger os ativos das organizações, é crucial adotar medidas efetivas e abrangentes.

Isso envolve implementar políticas de segurança robustas, realizar análises regulares de vulnerabilidade, aplicar patches e atualizações de segurança, além de monitorar e responder proativamente a possíveis incidentes de segurança.

Ao adotar uma abordagem abrangente e proativa para a segurança da informação, as organizações estarão mais preparadas para enfrentar os desafios e proteger seus ativos de forma eficaz.

No que diz respeito às estratégias de prevenção e resposta a incidentes, a maioria dos estudos sugere a adoção de medidas preventivas, tais como: implementação de firewalls, instalação de softwares de antivírus e antimalware, configurações de senhas fortes e atualização regular dos sistemas operacionais e softwares, além do uso de regras de acesso físico bem elaboradas.

É essencial estabelecer e manter estratégias efetivas para a resposta a incidentes, que incluem a identificação rápida do incidente, o isolamento do servidor

comprometido, a análise detalhada do incidente, a correção da vulnerabilidade explorada e a documentação cuidadosa do incidente para análises futuras. Essas estratégias devem ser incorporadas no Plano de Continuidade de Negócios (PCN), garantindo uma abordagem organizada e eficiente para lidar com incidentes de segurança da informação.

Em geral, os resultados obtidos mostram a importância da adoção de medidas preventivas e estratégias eficazes de resposta a incidentes em servidores on-premises, a fim de garantir a segurança da informação e proteger as empresas contra as ameaças e vulnerabilidades identificadas.

6 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo analisar as vulnerabilidades e ameaças em servidores on-premises e discutir as estratégias de prevenção e resposta a incidentes.

A análise da literatura realizada revelou que muitas vulnerabilidades podem ser corrigidas com medidas simples, enquanto as ameaças mais comuns exigem estratégias mais complexas de segurança.

No entanto, é importante ressaltar que este estudo possui algumas limitações. A pesquisa foi realizada através de uma análise bibliográfica, portanto, não foram coletados dados empíricos para análise. Portanto, a análise das estratégias de prevenção e resposta a incidentes não foi aprofundada em relação a cada ameaça específica.

Para futuras pesquisas, sugere-se a realização de estudos empíricos mais profundos que explorem as vulnerabilidades e ameaças em servidores on-premises, bem como a eficácia de diferentes estratégias de segurança na prevenção e resposta a incidentes.

É necessário um acompanhamento constante das vulnerabilidades e ameaças em servidores on-premises, bem como das soluções de segurança que podem ser aplicadas para garantir a proteção dos dados e sistemas.

Em suma, este estudo contribuiu para destacar a importância da segurança em servidores on-premises e a necessidade de implementação de medidas preventivas e estratégias eficazes de resposta a incidentes. Com a evolução constante das ameaças cibernéticas, é fundamental que as empresas adotem uma abordagem

abrangente e atualizada em relação à segurança da informação em seus servidores on-premises.

REFERÊNCIAS

2023 Cybersecurity Skills Gap. **Fortinet,** 2023. Disponível em: <https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf?utm_source=website&utm_medium=brpr&utm_campaign=cybersecurity-skills-gap-2023>. Acesso em: 04 jun. de 2023.

ANDERSON, Joy LePree. Global cyberattacks increased 38% in 2022. **Security Magazine**, 2023. Disponível em: <https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022>. Acessado em: 16 abr. de 2023.

Brasil é segundo país mais atingido por ciberataques na América Latina, diz relatório. **FEBRABAN TECH,** 2023. Disponível em: <https://febrabantech.febraban.org.br/temas/seguranca/brasil-e-segundo-pais-mais-atingido-por-ciberataques-na-america-latina-diz-relatorio>. Acesso em: 05 jun. de 2023.

CARNEIRO, Luciana; ALMEIDA, Maurício. Gestão da Informação e do Conhecimento no âmbito das práticas de Segurança da Informação: O fator humano nas organizações. Florianópolis: Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, 2013. 177 p. Disponível em: <https://www.redalyc.org/pdf/147/14729734010.pdf>. Acessado em: 08 dez. de 2022.

FARIA, Heitor M. **Bacula Ferramenta Livre De Backup**. [s.l.]: Brasport, 2010. 01 p. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=zzTV3Lutr4oC&oi=fnd&pg=PA1&dq=configura%C3%A7%C3%A3o+de+servidor+de+backup&ots=vtekImlG6A&sig=wbfQPi4MGSNoP2OMu2t6r0xfdK8#v=onepage&q=configura%C3%A7%C3%A3o%20de%20servidor%20de%20backup&f=false>. Acessado em: 04 dez. de 2022.

FERNANDES, Mirian. IDS e IPS: detecção e bloqueio de ameaças! **STARTI**, 2022. Disponível em: <https://blog.starti.com.br/ids-ips/>. Acessado em: 05 dez. de 2022.

FERNANDES, Mirian. Web Filter: por que a filtragem de navegação é importante? **STARTI**, 2022. Disponível em: <https://blog.starti.com.br/o-que-e-web-filter/>. Acessado em: 05 dez. de 2022.

FREITAS, Francisco Tércio de. A gestão da informação na área de segurança pública: gerenciamento eletrônico dos documentos e segurança da informação do centro integrado de operações de segurança pública - CIOSP-RN. Natal: Universidade Federal do Rio Grande do Norte, 2011. Disponível em:

<https://repositorio.ufrn.br/bitstream/123456789/39724/4/GestaoDaInformacao_Freitas_2011.pdf>. Acessado em: 16 abr. de 2023.

GALEGO, Nuno Miguel Carvalho; DUARTE, Nelson; MARTINHO, Domingos. Cloud Computing – Quem garante a segurança dos dados? Revista Eletônica: RISTI, 2022. Disponível em: <https://comum.rcaap.pt/bitstream/10400.26/43416/1/RISTI-PAPER.pdf>. Acessado em: 23 abr. de 2023.

GOGONI, Ronaldo. O que é proxy e qual a diferença para a VPN? **Tecnoblog**, 2019. Disponível em: <https://tecnoblog.net/responde/o-que-e-proxy-e-qual-a-diferenca-para-a-vpn/>. Acessado em: 05 dez. de 2022.

HINTZBERGEN, Jule et al. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Editora Brasport, 2018.

HYPERVISOR. **VMWare**, 2022. Disponível em: <https://www.vmware.com/br/topics/glossary/content/hypervisor.html#:~:text=Um%20hypervisor%2C%20tamb%C3%A9m%20conhecido%20como,recursos%2C%20como%20mem%C3%B3ria%20e%20processamento>. Acessado em: 02 dez. de 2022.

MACHADO, João V. Virtualização de servidores com software Hyper-V. Porto Alegre: Faculdade de Tecnologia Alcides Maya - AMTEC, 2019. 18 - 19 p. Disponível em: <http://raam.alcidesmaya.edu.br/index.php/projetos/article/view/104/103>. Acessado em: 03 dez. de 2022.

NEVES, Filipe; MACHADO, Leonardo; CENTENARO, Rodrigo. Implantação de firewall Pfsense. Curitiba: Universidade Tecnológica Federal do Paraná, 2014. 17 p. Disponível em: <http://repositorio.utfpr.edu.br/jspui/bitstream/1/9787/2/CT_COTEL_2014_2_02.pdf>. Acessado em: 05 dez. de 2022.

OLIVEIRA, Nairobi Spiecker de; et al. Segurança da Informação para Internet das Coisas (IoT): uma abordagem sobre a Lei Geral de Proteção de Dados (LGPD). São Leopoldo: Sociedade Brasileira de Computação – SBC, 2019. Disponível em: <https://sol.sbc.org.br/journals/index.php/reic/article/view/1704/1553>. Acessado em: 23 abr. de 2023.

OS melhores gerenciadores de senhas. **Cybernews,** 2022. Disponível em: <https://br.cybernews.com/lp/melhores-gerenciadores-de-senhas/?campaignId=14961831593&adgroupId=132066691641&adId=616858340062&targetId=kwd-369277346609&device=c&gunique=Cj0KCQiA1sucBhDgARIsAFoytUuGp-X8CGaqseR0lG1GCCw_HjQkZzqi3bJhj3xABmWmYQLt8JaSy6waAqzIEALw_wcB&gclid=Cj0KCQiA1sucBhDgARIsAFoytUuGp-X8CGaqseR0lG1GCCw_HjQkZzqi3bJhj3xABmWmYQLt8JaSy6waAqzIEALw_wcB>. Acesso em: 07 dez. de 2022.

POLÍTICA de segurança da informação. **Wikipédia,** 2021. Disponível em: <https://pt.wikipedia.org/wiki/Pol%C3%ADtica_de_seguran%C3%A7a_da_informa%C3%A7%C3%A3o>. Acesso em: 06 dez. de 2022.

RAMOS, Gabriel L. Segurança em ambientes virtualizados. Análise do comportamento de redes virtuais a ataques de rede. Brasília: Universidade de Brasília, 2019. 11 p. Disponível em: <https://bdm.unb.br/bitstream/10483/27849/1/2019_GabrielLucenaRamos_tcc.pdf>. Acessado em: 03 dez. de 2022.

SANTANA, Wesley. Sequestro de dados cresceu 13% no Brasil, mostra relatório da Sophos. **InfoMoney**, 2023. Disponível em: <https://www.infomoney.com.br/negocios/sequestro-de-dados-cresceu-13-no-brasil-mostra-relatorio-da-sophos/amp/>. Acessado em: 17 mai. de 2023.

SANTOS, Eduardo Esteves dos; SOARES, Tamires Mariana Mayumi Kurosaki; GIRALDI, Marcus Vinícius Lahr. Riscos, ameaças e vulnerabilidades: o impacto da segurança da informação nas organizações. Americana: FATEC Americana, 2018. Disponível em: <http://ric.cps.sp.gov.br/bitstream/123456789/3255/1/20182S_SANTOSEduardoEstevesdos_OD0529.pdf>. Acessado em: 12 mar. de 2023.

SEGURANÇA em ambientes virtualizados. **DEVMEDIA**, 2014. Disponível em: <https://www.devmedia.com.br/hypervisor-seguranca-em-ambientes-virtualizados/30993>. Acessado em: 02 dez. de 2022.

SILVA, Bruno. Dia Mundial da Senha: Brasileiros ignoram riscos e insistem na utilização de chaves fracas. **Security Report**, 2022. Disponível em: <https://www.securityreport.com.br/destaques/dia-mundial-da-senha-brasileiros-ignoram-riscos-e-insistem-na-utilizacao-de-chaves-fracas/#.ZGeWg3bMLIV>. Acessado em: 16 abr. de 2023.

VALE, André Luiz Mariano do. Monitoramento de redes: a importância do monitoramento de redes para a segurança da informação. Natal: Universidade do Sul de Santa Catarina - UNISUL, 2017. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/9005/1/%5b45471-47484%5dtemplate_estudo_de_caso_novo_2016%2017-09-18%2017-21%20-%20AD3.pdf>. Acessado em: 12 mar. de 2023.

WANGENHEIM, Aldo von et al. Autenticação Multi-Fator Para Telemedicina Usando Dispositivos Móveis E Senhas Descartáveis. Goiânia: Congresso Brasileiro de Informática em Saúde - CBIS, 2016. Disponível em: <https://docs.bvsalud.org/biblioref/2018/07/906776/anais_cbis_2016_artigos_completos-1041-1050.pdf >. Acessado em: 7 mai. de 2023.

ZEQUIM, Eduarda Pagim; RIBEIRO, Douglas Francisco. O Papel Da Inteligência Artificial Na Segurança Cibernética. Taquaritinga: Revista Interface Tecnológica, 2022. Disponível em:

<https://revista.fatectq.edu.br/interfacetecnologica/article/view/1358/748>. Acessado em: 23 abr. de 2023.