Modelagem de Ameaças Aplicada à Segurança Física de Datacenter: uma Revisão Bibliométrica

Edson Nunes[1], Napoleão Galegale[2];

Resumo**:** Este artigo tem como objetivo verificar se há na literatura *frameworks* para modelagem de ameaças voltadas à segurança física de um Datacenter. A metodologia utilizada foi qualitativa baseada no protocolo PRISMA P. Foi identificado que há oportunidade para o desenvolvimento e aplicação de *frameworks* voltados a modelagem de ameaças aplicada à segurança física de um datacenter, contribuindo para reduzir possíveis riscos de ameaças desta natureza, além de contribuir para preencher a lacuna existente na literatura e apoiar a comunidade profissional.

Palavras-chave: Datacenter. Segurança da informação. Segurança física. Modelagem Ameaças.

Abstract: This article aims to verify if there are frameworks in the literature for modeling threats aimed at the physical security of a Datacenter. The methodology used was qualitative based on the PRISMA P protocol. It was identified that there is an opportunity for the development and application of frameworks aimed at modeling threats applied to the physical security of a datacenter, contributing to reduce possible risks of threats of this nature, in addition to helping to fill the gap in the literature and support the professional community.

Keywords: Datacenter. Information security. Physical security. Modeling Threats.

1 Introdução

Este artigo científico refere-se a um estudo bibliométrico baseado em modelagem de ameaças aplicada à segurança em um datacenter, que é essencialmente uma representação estruturada de todas as informações que afetam a segurança de um ativo ou sistema. Uma ameaça é um evento indesejável que pode ocorrer incidental como uma falha de um dispositivo de armazenamento.

A modelagem de ameaças permite a tomada de decisões informadas sobre o risco de segurança de um determinado ativo ou sistema. Além de produzir um modelo, os esforços de uma modelagem de ameaças também produzem uma lista priorizada de melhorias de segurança para o conceito, requisitos, design ou implementação de ativos em um datacenter.

A modelagem de ameaças físicas à um datacenter tem como objetivo identificar vulnerabilidades para definir contramedidas para prevenir ou mitigar os

efeitos de ameaça física a um ativo e identificar os requisitos de segurança em ambientes de missão crítica na qual possuem dados valiosos. É um processo sistemático e estruturado que propõe identificar potenciais ameaças e vulnerabilidades para reduzir o risco aos recursos de TI. Também ajuda os gerentes de TI a entender o impacto das ameaças, quantificar sua gravidade e implementar controles. Uma metodologia de modelagem de ameaças é uma maneira de dividir um processo complexo em tarefas menores, facilitando a identificação de pontos fracos.

Qualquer ativo em uma infraestrutura de um Datacenter deve ser projetado para resistir a falhas, mas estabelecer os requisitos de segurança necessários para este alcance torna-se complexo. A importância da modelagem de ameaças voltada à segurança física é um processo que ganha cada vez mais visibilidade dentro das equipes de TI. Com a transformação digital, para a proteção dos ativos e por consequência dos negócios, é necessário um trabalho muito mais aprofundado e elaborado.

A modelagem de ameaças abrange cenários de forma muito mais holística. Não se trata de conscientização de segurança. Sua abrangência é mais completa, podendo fornecer ao gestor um panorama sobre toda a parte física de um datacenter, deixando claro se a equipe de TI está ou não preparada para agir .

A modelagem de ameaças voltada à segurança física não é exclusiva de infraestruturas de maduras e robustas. Mesmo as pequenas e médias empresas podem ter bons resultados trabalhando em algumas etapas básicas para identificar alguns pontos cegos importantes. Se aplicada a modelagem de ameaças à parte física e de forma inicial, o gestor de TI poderá amadurecê-la e torná-la mais eficaz à medida que o setor cresce, aumentando seus recursos e disponibilidade.

Existem várias estruturas e metodologias de modelagem de ameaças encontram-se aplicáveis à segurança física de um datacenter, no entanto, as etapas principais são semelhantes em sua maioria e com a seguinte composição:

a) Formação de uma equipe: Essa equipe deve incluir todas as partes interessadas, incluindo gestores de TI e colaboradores que atuam na infraestrutura do datacenter. Uma equipe diversificada irá gerar um modelo de ameaça mais holístico.
b) Estabelecer um escopo: Definir um modelo, criar um inventário de todos os componentes físicos e classificá-los.
c) Determinar ameaças prováveis: Para todos os componentes que são alvos de ameaças, determinar onde existem ameaças. Esta ação ajudar a criar cenários de ameaças amplos, técnicos e inesperados, podendo identificar possíveis vulnerabilidades ou fraquezas que podem levar ao comprometimento ou falha dos componentes físicos.
d) Classificar cada ameaça: Determinar o nível de risco que cada ameaça física representa e classificá-la para priorizar a mitigação de riscos. Uma abordagem eficaz é multiplicar o potencial de dano de

uma ameaça física pela probabilidade de sua ocorrência dentro de um datacenter.

e) Implementar mitigações: Decidir como mitigar cada ameaça ou reduzir o risco a um nível aceitável. As opções são evitar o risco, transferi-lo, reduzi-lo ou aceitá-lo.
f) Documentar: Documentar as descobertas e ações, para que futuras alterações nos ativos de um datacenter possam ser avaliados rapidamente e o modelagem de ameaças atualizada.

Metodologias e estruturas de modelagem de ameaças

As primeiras metodologias de modelagem usavam diagramas de fluxo de dados para visualizar como os dados se movem em um aplicativo ou sistema. No entanto eram muito limitados para aplicativos modernos que são implantados em ambientes altamente interconectados com vários usuários e dispositivos interconectados.

Os diagramas de fluxo do processo agora são comumente usados. Apresentam um aplicativo ou sistema da perspectiva das interações do usuário e como invasores em potencial podem tentar se mover através do aplicativo. Isso torna mais fácil identificar e priorizar ameaças potenciais.

As árvores de ataque também são usadas para visualizar ataques a um sistema, a árvore de causas sendo o objetivo de um ataque, com as folhas sendo os meios pelos quais um ataque pode atingir esse objetivo. As árvores de ataque podem ser construídas para componentes individuais de um aplicativo ou para avaliar um tipo específico de ataque.

Muitas metodologias e estruturas de modelagem de ameaças foram desenvolvidas. Os centrados em ataques concentram-se nos tipos de ataques possíveis e os centrados em ativos concentram-se nos ativos que necessitam de proteção. Os mais comuns usam as seguintes abordagens:

- Danos, reprodutibilidade, explorabilidade, usuários afetados, detectabilidade (*DREAD – Damage, Reproducibility, Exploitability, Affected users, Discoverability*) é uma análise de risco quantitativa que classifica, compara e prioriza a gravidade de uma ciberameaça.
- O Guia do NIST (*National Institute of Standards and Technology*) para Modelagem de Ameaças de Sistema Centrado em Dados (*Data-Centric System Threat Modeling*) concentra-se na proteção de tipos de dados específicos dentro dos sistemas e modela aspectos de ataque e defesa para dados selecionados.
- A Avaliação de Ameaças, Ativos e Vulnerabilidades Operacionalmente Críticas (*OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation*) fornece avaliação estratégica baseada em ativos e riscos visando objetivos de segurança específicos e gerenciamento de riscos. Foi desenvolvida pela *Carnegie Mellon University* para o Departamento de Defesa.

- O Processo de Simulação de Ataque e Análise de Ameaças (*PASTA – Process for Attack Simulation and Threat Analysis*) é um processo de sete etapas, centrado no ataque, projetado para correlacionar requisitos técnicos com objetivos de negócios, considerando a análise de impacto nos negócios e requisitos de conformidade.
- *STRIDE* faz parte do Ciclo de Vida de Desenvolvimento de Segurança da Microsoft. Identifica entidades do sistema, eventos e limites e, em seguida, aplica um conjunto de ameaças conhecidas. Usando-o, as equipes de segurança podem identificar ameaças potenciais.
- *Trike* é uma metodologia de código aberto centrada no risco que garante que o nível de risco atribuído a cada ativo esteja OK para todas as partes interessadas.
- *Visual, Agile, and Simple Threat (VAST*) é baseado no *ThreatModeler*, uma ferramenta automatizada de modelagem de ameaças projetada para se integrar a um ambiente de desenvolvimento de software *Agile* e fornecer resultados acionáveis para desenvolvedores e equipes de segurança.

Como benefício e atuando da maneira certa, uma modelagem de ameaças aplicada à segurança física de um datacenter permite que as decisões de segurança sejam tomadas de forma racional. O processo de modelagem de ameaças naturalmente produz um argumento de garantia que se empregado, pode proteger a segurança aos componentes físicos.

O processo de modelagem de ameaças voltada à segurança física deve ser repetido sempre que a infraestrutura de TI ou o ambiente de ameaças forem alterados. Isso mantém o modelo de ameaça atualizado, à medida que novas ameaças surgem.

O valor de um data center não pode ser mensurado apenas pelo valor de seus equipamentos. Associadas ao data center, estão todas as informações da empresa como, por exemplo, a compra de matéria prima, entre outros.

Muitas empresas possuem como negócio principal a venda de produtos pela internet. Esse serviço não existiria sem o funcionamento de data centers de alta disponibilidade.

Os danos gerados pela perda ou interrupção desses dados não só podem influenciar a empresa de forma financeira, mas também podem danificar de maneira irreversível a imagem da instituição frente ao seu mercado de atuação.

Marconi e Lakatos (2010) afirmam que uma pesquisa, para ser realizada, requer a definição clara e objetiva de um problema que motive sua realização. Deste modo, a questão base investigada compreende: Uma nova modelagem de ameaças físicas a um datacenter sendo tratada como metodologia a ser implantada para uma organização.

Diante deste contexto, este artigo tem como principal objetivo responder a seguinte questão de pesquisa: Há *frameworks* na literatura para modelagem de ameaças voltadas à segurança física de datacenter?

Para alcançar esta questão, foram definidos os seguintes objetivos: efetuar uma bibliometria; fazer a revisão da literatura; realizar a análise qualitativa dos documentos selecionados. A partir desta questão de pesquisa, apresentam-se duas proposições:

P1) Há a oportunidade para o desenvolvimento e aplicação de *frameworks* voltados para a modelagem de ameaças aplicada à segurança física de um datacenter.

P2) Não há a oportunidade para o desenvolvimento e aplicação de *frameworks* voltados para a modelagem de ameaças aplicada à segurança física de um datacenter.

O estudo bibliométrico servirá de base para levantamento do material propondo-se uma modelagem de ameaças baseada em segurança física, e com seus resultados, apresentar sua importância na comunidade profissional e acadêmica de forma expressiva.

2 Referencial Teórico

Uma pesquisa global em segurança da informação realizada pela empresa PWC (2014), constatou que a informação tem sido considerada um dos ativos mais valiosos da empresa. Esse valor é proveniente tanto pelo conhecimento que a informação traz, como também pela pronta aplicação dessa informação no processo decisório (TURBAN; VOLONINO, 2013).

Este trabalho problematiza a busca de melhorias de segurança física de datacenters, uma vez que o comprometimento das informações armazenadas nestes locais pode gerar perdas de grande valia para tais organizações, ameaçando inclusive a sua sustentabilidade (TURBAN; VOLONINO, 2013).

Todo ativo em um ambiente de missão crítica tem indicações de manutenção recomendadas pelo fabricante ou uma melhor prática para a manutenção. É importante entender que os planos de manutenção não são todos iguais. Faz-se necessário um programa com manutenções preventivas, preditivas e corretivas, rastreadas dentro do mesmo sistema de controle para garantir que as informações estejam disponíveis para a implementação e elaboração de relatórios.

Uma vez que toda a manutenção é incluída em um cronograma, cada item necessitará de um procedimento aprovado e revisado que cubra a execução da manutenção, bem como a operação dos sistemas, garantindo que nenhuma condição inesperada cause impacto negativo no ambiente crítico.

O Datacenter é uma estrutura física, sendo edifício ou parte de um edifício, projetado para abrigar uma variedade de recursos que fornecem armazenamento e gerenciamento de equipamentos de rede, servidores e telecomunicação. Segundo Marin (2011), um datacenter compreende um ambiente no qual estão equipamentos que armazenam informações críticas para a continuidade do negócio de uma ou mais organizações, independentemente do setor em que atuam.

Para Paloalto (2016), um Datacenter centraliza as operações de TI de uma empresa, armazenando e gerenciando seus dados. Nesse sentido, há normas específicas para determinar os critérios de segurança dos Datacenters, entre essas a ANSI/TIA-942. A TIA (*Telecommunications Industry Association*) é uma organização que representa a indústria da informação e da comunicação global de tecnologia, desenvolvendo normas, iniciativas políticas, oportunidades de negócios, inteligência de mercado, e eventos, tendo seu foco em melhorias em telecomunicações, internet, cabeamento, satélites, e credenciada pela ANSI (*American National Standardas Institute*) (ANSI/TIA-942, 2005).

De acordo com Veras (2009), a ANSI/TIA-942 é uma norma que especifica os requisitos mínimos para a infraestrutura de Datacenters, de acordo com o grau de disponibilidade e redundância de sua infraestrutura.

Modelar ameaças é uma gestão de riscos, na conscientização sobre quais medidas de segurança devem ser adotadas e em facilitar a tradução de aspectos técnicos dos sistemas e processos em impactos de negócio que podem ocorrer caso alguma ameaça analisada seja materializada (Howard & Lipner, 2006).

Nenhuma aplicação consegue garantir 100% de segurança ao ser exposta a ambientes hostis e complexos. A solução é saber sobre a presença das ameaças para que se possa gerenciar os riscos adequadamente. Em última instância, a modelagem de ameaças permite aumentar o retorno de investimento ao se concentrar nas questões relevantes sobre a segurança de um sistema (Microsoft Technet, 2004).

De forma mais abrangente, Oladimeji, Supakkul e Chung (2006), apontam que a modelagem de ameaças permite revisar a arquitetura de um sistema, identificar e analisar suas ameaças, projetar contramedidas de segurança e orientar os testes de segurança ao qual um sistema deverá ser submetido. Isto é possível ao examinar os sistemas sob o ponto de vista de um adversário em potencial (ameaça), identificando os maiores riscos aos quais os sistemas estão expostos (Ibidem).

3 Método

A metodologia proposta para este artigo foi qualitativa e como base para o referencial teórico utilizou-se as bases *Web os Science* e *Scopus* para obtenção de material.

Sintaxe utilizado na *Web of Science*:

“threat modeling" OR "threat model" (Todos os campos) and "Physical security" OR "data center" OR "datacenter" (Todos os campos) and Computer Science Information Systems or Computer Science Theory Methods or Computer Science Hardware Architecture or Computer Science Software Engineering **or** Engineering Electrical Electronic (Categorias da Web of Science)

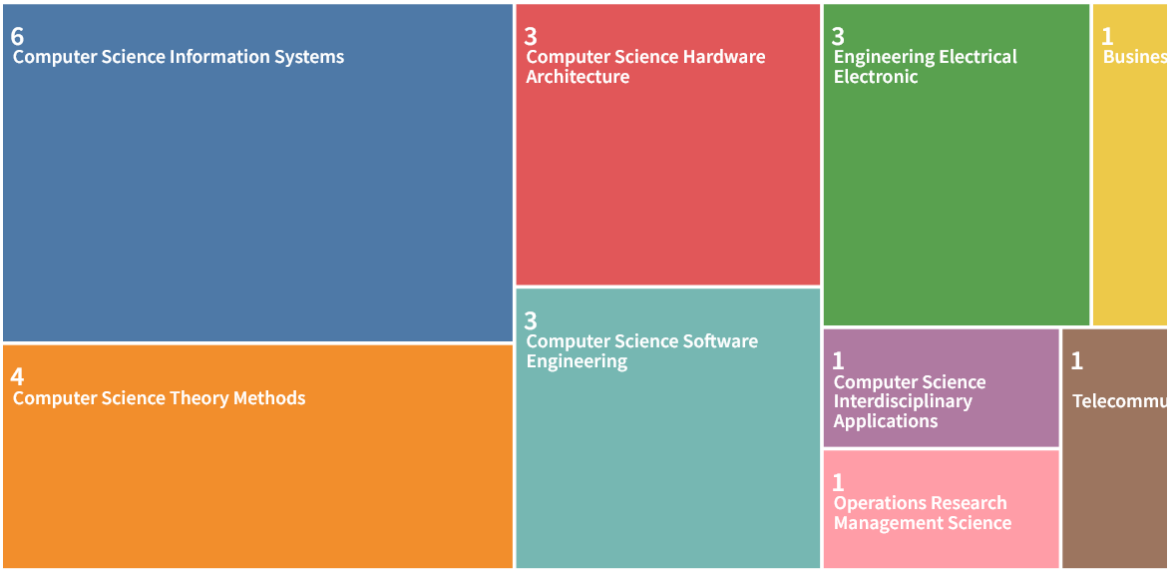

Gráfico 1 – Áreas de pesquisa
Fonte: o autor

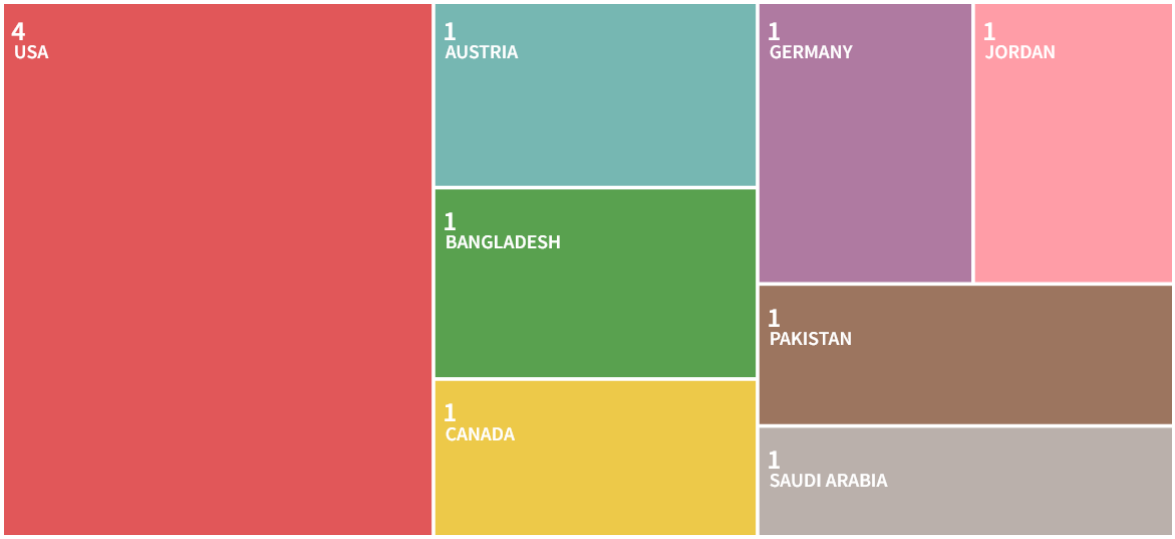

Gráfico 2 - Países
Fonte: o autor

Gráfico 3 – Concentração das editoras
Fonte: o autor

Sintaxe utilizada na base *Scopus*:

ALL ("Threat modeling" OR "threat model" AND "Physical security" OR "data center" OR "datacenter") AND (LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014) OR LIMIT-TO (PUBYEAR , 2013) OR LIMIT-TO (PUBYEAR , 2012) OR LIMIT-TO (PUBYEAR , 2011)) AND (LIMIT-TO (SUBJAREA , "COMP")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (EXACTSRCTITLE , "IEEE Access") OR LIMIT-TO (EXACTSRCTITLE , "Security And Communication Networks") OR LIMIT-TO (EXACTSRCTITLE , "Computers And Security") OR LIMIT-TO (EXACTSRCTITLE , "Computer Communications"))

Período: Últimos 10 anos.

Resultado: 395 artigos.

A triagem e seleção dos artigos baseia-se no protocolo PRISMA P, que foi desenvolvido como um roteiro para apoiar pesquisadores na realização de revisões sistemáticas e meta-análises que retornem um conjunto mínimo de itens importantes a serem considerados no protocolo de pesquisa (Moher et al.,2015).

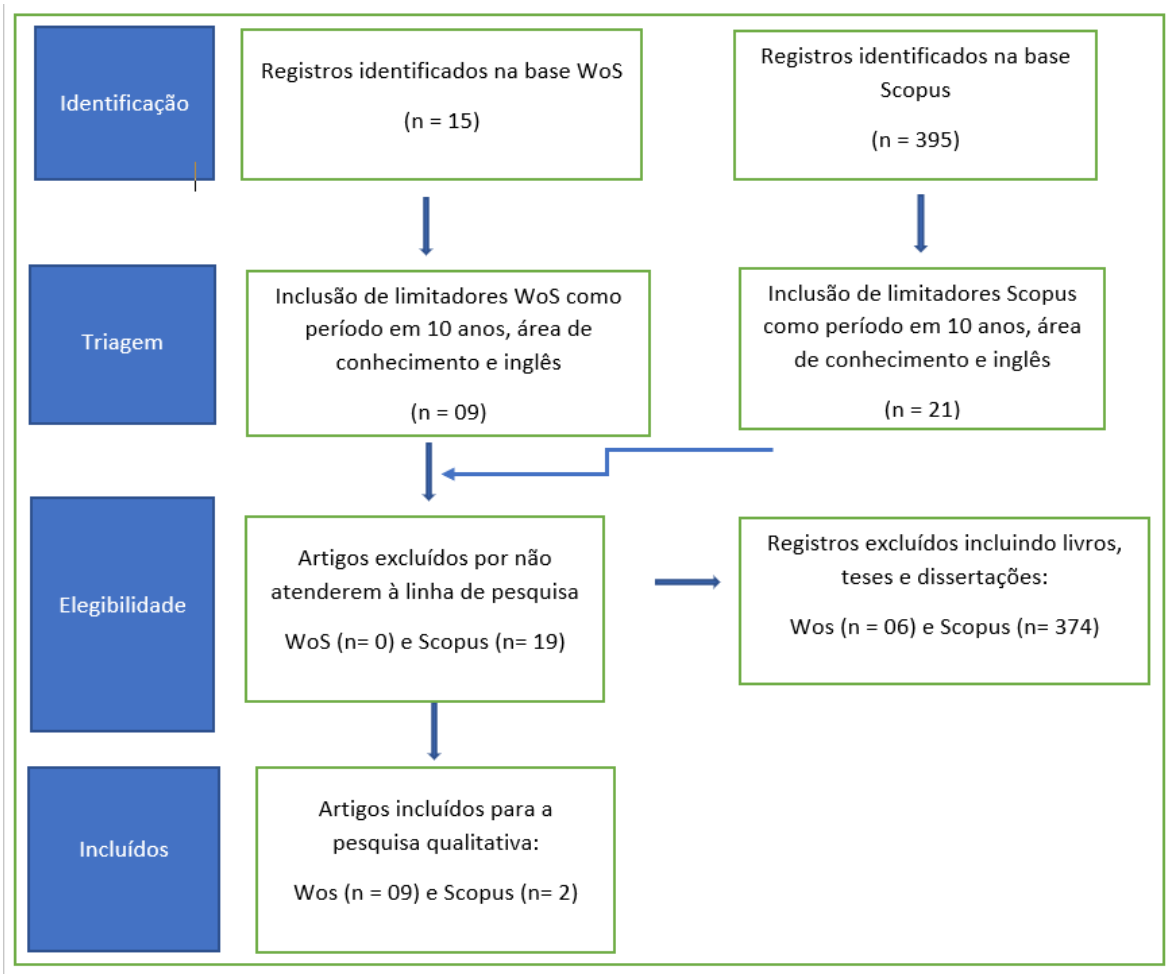

Figura 1 – Fluxograma da pesquisa

Fonte: Adaptado de Moher et al. (2015).

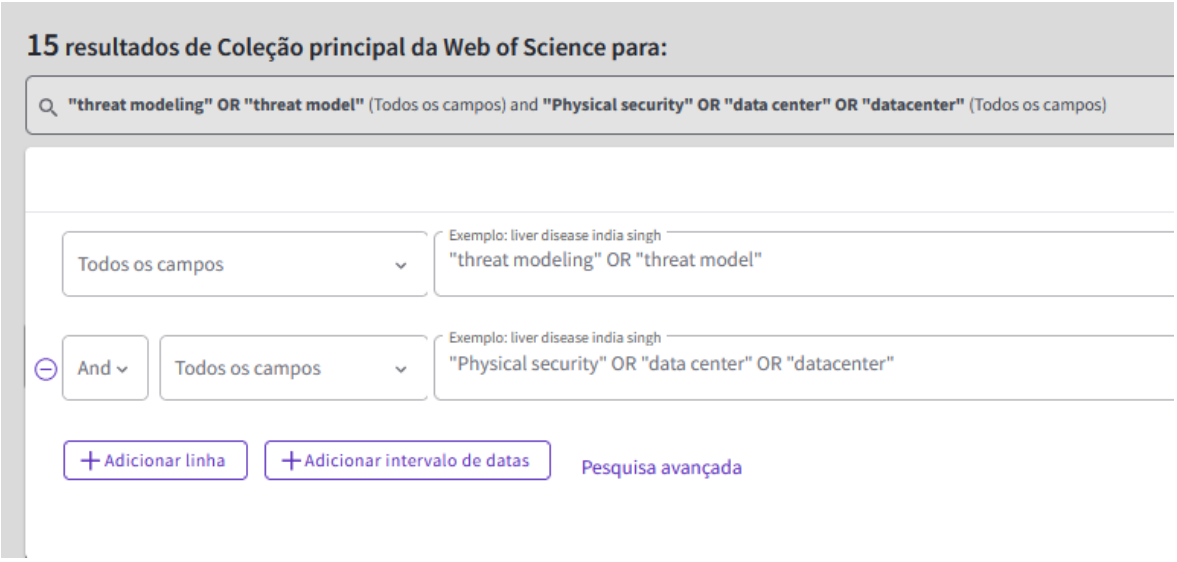

Figura 2 – Critérios de busca no *Web of Science*

Fonte: Resultado da Pesquisa.

Inicialmente a busca retornou 15 resultados, onde na figura 3 apresenta-se uma nova limitação, incluindo áreas de conhecimento buscando manter o perímetro à pesquisa, obtendo um novo resultado com 9 artigos.

Áreas de conhecimento:

a) *Computer Science Information Systems*
b) *Computer Science Theory Methods*
c) *Computer Science Hardware Architecture*
d) *Computer Science Software Engineering*
e) *Engineering Electrical Electronic*

Figura 3 – Inclusões no critério de busca

Fonte: Resultado da Pesquisa.

No momento da triagem para a base Scopus foram aplicados os limitadores como período de 10 anos, limitando-se à língua inglesa e usando *Computer Communications* como a área de conhecimento, limitando-se a 21 artigos.

No momento da elegibilidade para a base *Web of Science* foram excluídos 06 registros e mantidos os 9 artigos e na base *Scopus* foram excluídos livros, teses e dissertações, resultando em 374 artigos deletados e mantidos 21 artigos.

Ainda como elegibilidade, foram removidos artigos não adequados à linha de pesquisa resultando em:

Web of Science: 0 deletados e 9 mantidos

Scopus: 19 deletados e 2 mantidos

Fixado este valor final, foi realizada a leitura integral e criteriosa de todos os artigos para a realização da análise qualitativa, cujo resultado aplicado no próximo tópico: Resultados e Discussão.

4 Resultados e Discussão

Ao analisar de forma criteriosa o conteúdo os 11 artigos filtrados na etapa de bibliometria, apresenta-se uma lacuna para investigação, uma vez que os artigos

publicados tratam os estudos a seguir, mas não o objeto de pesquisa: a modelagem de ameaças aplicada à segurança física de um datacenter.

Ao analisar o artigo "Uma estrutura para realizar a segurança sob demanda na computação em nuvem", apresenta-se segurança em nuvem sob demanda, permitindo diferenciação e preços competitivos ao cliente, com base em um modelo de ameaça que corresponda à segurança contratada.

O artigo "Mitigação de ameaças internas em nuvem usando uma abordagem da base de conhecimento enquanto mantida a disponibilidade dos dados" analisa uma modelagem de ameaças interna em um data center em nuvem em seus vários níveis como host, redes, banco de dados e sistemas, mas sem citar meios e/ou formas de modelagem de ameaças aplicada à segurança física.

Ao analisar o artigo "Abordagem da Análise de segurança para integrar *middleboxes* em redes definidas por software", o mesmo traz a abordagem de Rede definida por software (SDN), apresentando o gerenciamento de redes corporativas e de data centers com facilidade, junto com a integração de *middleboxes*, que fornece funções de rede que são cruciais para a segurança, desempenho e confiabilidade, e com novos desafios, por exemplo, por meio de *middleboxes* em uma determinada ordem tornando o roteamento mais complexo. Este tipo de modelagem, se não aplicadas determinadas políticas de forma correta, podem trazer falhas de design em sua arquitetura que podem levar a vulnerabilidades graves e colocar a segurança da rede e datacenter.

Já o artigo "Análise comparativa de segurança de redes sem fio definidas por software (SDWN) - protocolos BGP e NETCONF", apresenta os riscos em data centers com redes gerenciadas por software e sua complexidade, onde suas vulnerabilidades são constantes necessitando de monitoração adequada para combater ataques à serviços.

O artigo seguinte analisado: "Modelagem de ameaças para infraestruturas de data center em nuvem", apresenta a transição de data centers tradicionais para a nuvem devido à sua flexibilidade e menor custo, com exercícios de modelagem de ameaças usando métodos populares de ataques aos dados e lições práticas para que um provedor possa avaliar, entender e implantar soluções, mas sem citar meios e/ou formas de modelagem de ameaças aplicada à segurança física.

Com base na bibliometria, apresenta-se o artigo “Sistema de Sinalização 7 (SS7): Limitações e Resoluções”, que é um meio pelo qual elementos da rede telefônica trocam informações. Esta tecnologia faz menção à década de 1970, época em que os protocolos de segurança dependiam da segurança física dos hosts e da comunicação via canais. No início do século 21, mecanismos mais recentes permitiram o uso de redes IP para transferência de mensagens e mesmo com essas novidades, vulnerabilidades permanecem dentro dos protocolos SS7, onde é explorado neste artigo pontos fracos e modelagem de ameaças para tal protocolo.

Já o artigo "Integrando modelagem de ameaças e automação de casos de teste em testes de segurança de software industrializados” objetiva detalhar a

lacuna entre a modelagem de ameaças e a geração automatizada de casos de teste na indústria. Se concentra na análise do aplicativo *Industrial Internet of Things (IIoT)*, usado para impulsionar a eficiência da produção industrial, com maior integração entre sistemas, mas não projetado como amplamente acessível e interoperável, trazendo infinitas ameaças.

Avaliou-se o artigo "Estrutura de modelagem de ameaças para segurança de armazenamentos unificados em Data Center privados" que objetiva atender vulnerabilidades e ameaças juntamente com mitigações, em nível de *Storage* em um data center privado, com ampla aceitação de mercado, mas com potenciais riscos para o cliente como perda de dados. Enfatiza-se que este artigo teve sua limitação à ativos de *Storage* e não a um Datacenter como um todo.

Com a avaliação do artigo "Detecção e forense contra falsificação de dados furtivo na infraestrutura de medição inteligente", apresentando uma modelagem de ameaças para este universo logico e físico, baseado em dados de consumo de energia falsos e injetados em medidores por meio de redes inteligentes, sendo uma ameaça que afeta negativamente tanto para o cliente quanto empresas/utilitários.

Avaliando o artigo “Implementação de um sistema ciberfísico em tempo real”, apresenta uma modelagem de ameacas de cyber ataques a redes inteligentes acoplando sistemas de energia modernos, mas nao detalhando ameaças fisicas a uma rede física.

Por fim, ao avaliar o artigo “Uma Pesquisa sobre Controle de Acesso em Computacao em Névoa”, traz a atrativa solução para aplicações em *IoT*, com baixa latência e serviços altamente móveis e distribuídos geograficamente, buscando uma modelagem de ameaças para este ambiente no quesito controle de acessos, mas nao apresentando relacionamento quanto a dificuldades fisicas.

A avaliação demonstra que a modelagem tratada está ligada às tecnologias como Sistemas Ciber-Fisicos (CPS), Computação em nuvem (*cloud*), Redes e Internet das Coisas (*IoT*), com a lacuna para investigação: a modelagem de ameaças aplicada à segurança física de um datacenter.

5 Considerações finais

Esta pesquisa sobre Modelagem de Ameaças aplicada à Segurança física de um Datacenter problematiza a busca de melhorias de segurança física de Datacenters, uma vez que o comprometimento das informações armazenadas nestes locais pode gerar perdas de grande valia para tais organizações, ameaçando inclusive a sua sustentabilidade (TURBAN; VOLONINO, 2013).

O resultado geral desta pesquisa confirma a proposição P2 nos objetivos específicos propostos, onde realizou-se a bibliometria para obtenção de artigos, efetuada a revisão da literatura e ao analisar de forma qualitativa os dados obtidos evidencia-se a sua limitação, onde não foi localizado nenhum artigo propondo um *framework* para modelagem de ameaças aplicada à segurança física, assim

surgindo lacunas nesta abordagem e apresentando a oportunidade para estudos futuros e aprofundamento no tema.

A contribuição desta pesquisa é a exploração dos dados apresentados, servindo de referência a pesquisadores para futuramente detalharem o tema e sua respectiva literatura.

Referências

A. Amini, N. Jamil, A.R. Ahmad and M.R. Z`aba, 2015. Threat Modeling Approaches for Securing Cloud Computin. Journal of Applied Sciences, 15: 953-967. DOI: 10.3923/jas.2015.953.967 URL: https://scialert.net/abstract/?doi=jas.2015.953.967

A. I. Swapna, M. R. Huda and M. K. Aion, "Comparative security analysis of software defined wireless networking (SDWN)-BGP and NETCONF protocols," 2016 19th International Conference on Computer and Information Technology (ICCIT), 2016, pp. 282-287, doi: 10.1109/ICCITECHN.2016.7860210.

B. Chen, K. L. Butler-Purry, A. Goulart and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," 2014 North American Power Symposium (NAPS), 2014, pp. 1-6, doi: 10.1109/NAPS.2014.6965381.

Howard, M., & Lipner, S. The Security Development Lifecycle. Redmond, Washington: Microsoft Press, 2006.

Stefan Marksteiner, Rudolf Ramler and Hannes Sochor, "Integrating threat modeling and automated test case generation into industrialized software security testing", *Proceedings of the Third Central European Cybersecurity Conference CECC*, 2019.MARIN, P. S. Datacenters: desvendando cada passo: conceitos, projetos, infraestrutura física e eficiência energética. 1. Ed. São Paulo: Érica, 2011

Microsoft Technet. Modelagem de Ameaças de Segurança. Janeiro de 2004. Disponível em: http://technet.microsoft.com/pt-br/library/dd569893.aspx. Acesso em 30 de junho de 2022.

Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., Stewart, L. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Syst Rev* **4**, 1 (2015). https://doi.org/10.1186/2046-4053-4-1

Oladimeji, E. A., Supakkul, S., & Chung, L. Security Threat Modeling And Analysis: A Goal-Oriented Approach. 8, 2006.

P. Jamkhedkar, J. Szefer, D. Perez-Botero, T. Zhang, G. Triolo and R. B. Lee, "A Framework for Realizing Security on Demand in Cloud Computing," 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, 2013, pp. 371-378, doi: 10.1109/CloudCom.2013.55.

P. Patel and S. Acharya, "Signaling System 7: Limitations and Resolutions," 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2018, pp. 1-6, doi: 10.1109/ANTS.2018.8710116.

PALOALTO. O que é um datacenter. [s.d]. Disponível em: https://www.paloaltonetworks.com.br/resources/learning-center/what-is-a-data-center.html. Acesso em: 01 jul. 2022.

P. Zhang, J. K. Liu, F. R. Yu, M. Sookhak, M. H. Au and X. Luo, "A Survey on Access Control in Fog Computing," in IEEE Communications Magazine, vol. 56, no. 2, pp. 144-149, Feb. 2018, doi: 10.1109/MCOM.2018.1700333.

Q. Althebyan, R. Mohawesh, Q. Yaseen and Y. Jararweh, "Mitigating insider threats in a cloud using a knowledgebase approach while maintaining data availability," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pp. 226-231, doi: 10.1109/ICITST.2015.7412094.

S. Bhattacharjee and S. K. Das, "Detection and Forensics against Stealthy Data Falsification in Smart Metering Infrastructure," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, pp. 356-371, 1 Jan.-Feb. 2021, doi: 10.1109/TDSC.2018.2889729.

S. M. Hussain, M. H. Islam, A. Ali and M. U. Nazir, "Threat Modeling Framework For Security Of Unified Storages In Private Data Centers," 2020 IEEE 22nd Conference on Business Informatics (CBI), 2020, pp. 111-120, doi: 10.1109/CBI49978.2020.10068

T. Eggert and R. Khondoker, "Security analysis of approaches to integrate middleboxes into software defined networks," 2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), 2016, pp. 1-7, doi: 10.1109/CEEICT.2016.7873055.

M. Veras, "Datacenter: Datacenter: Componente Central da Infraestrutura de TI" in , Rio de Janeiro:Brasport, 2009.