ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 12, Issue, 04, pp. 55049-55055 April, 2022
https://doi.org/10.37118/ijdr.24250.04.2022

RESEARCH ARTICLE OPEN ACCESS

MODELAGEM DE AMEAÇA, ANÁLISE DE RISCO E SUAS APLICAÇÕES NA LITERATURA

***[1]Rodrigo Yokoyama and [2]Carlos Hideo Arima**

[1]Mestrando do Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, Centro Estadual de Educação Tecnológica Paula Souza, Brasil; [2]Professor e pesquisador do Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, Centro Estadual de Educação Tecnológica Paula Souza, Brasil

ARTICLE INFO

Article History:
Received 27th January, 2022
Received in revised form
09th February, 2022
Accepted 20th March, 2022
Published online 22nd April, 2022

Key Words:
Análise de Risco, Avaliação de Risco, Identificação de Risco, Modelagem de Ameaça.

****Corresponding author: Rodrigo Yokoyama,***

ABSTRACT

Entre os processos existentes para avaliação de risco, modelagem de ameaça é um processo relacionada a gestão de risco. Modelagem de ameaça é uma técnica que visa a melhoria contínua da segurança de um ambiente, na construção ou manutenção de um software ou implantação de novas tecnologias. Realizou-se uma análise textual utilizando como base, o trabalho publicado pelo Shostack, considerado como referência no assunto de modelagem de ameaça, posteriormente realizou-se uma análise bibliométrica utilizando as palavras com maior reincidência do livro. Com base nos artigos encontrados, realizou-se uma verificação sobre os temas abordados pelos artigos e foram encontrados os modos de como o tema de modelagem de ameaça é abordado, técnicas utilizadas e de que modo é empregado. Após análise dos artigos encontrados, foi possível identificar as técnicas utilizadas e apresentadas por cada artigo e afirmar a proposição de que STRIDE é a técnica predominante dentro da literatura entre as outras técnicas encontradas.Com base nas aplicações de modelagem de ameaça apresentadas pelos artigos encontrados, nota-se que há uma grande variedade de áreas que podem ser beneficiadas com a implementação da prática de modelagem de ameaça.

Citation: ***Rodrigo Yokoyama and Carlos Hideo Arima.*** "Modelagem de ameaça, análise de risco e suas aplicações na literatura", *International Journal of Development Research*, 12, (04), 55049-55055.

INTRODUCTION

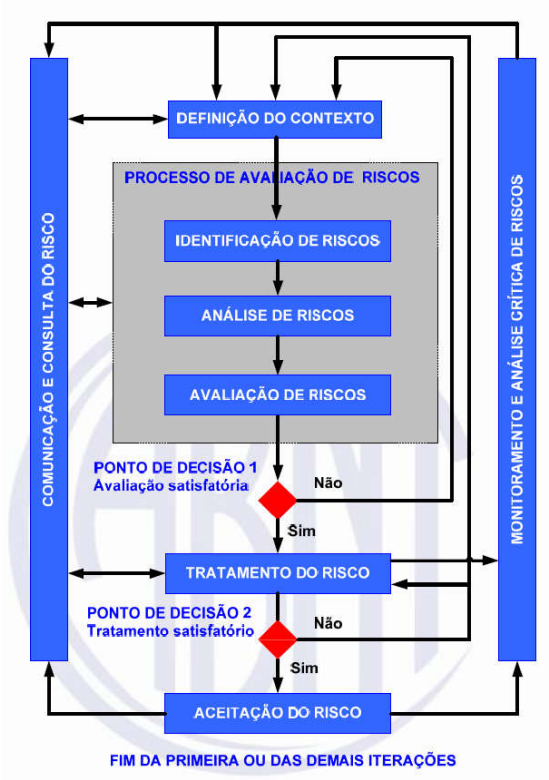
Entre os processos existentes para avaliação de risco, modelagem de ameaça é um processo relacionada a gestão de risco. Modelagem de ameaça é uma técnica utilizada que está em ascensão no ambiente acadêmico, visa a melhoria contínua de um ambiente, na construção ou manutenção de um software, implantação, manutenção ou adoção de novas tecnologias e soluções, auxiliando em assuntos relacionados à segurança da informação. Conforme pesquisa realizada sobre o assunto utilizando o site Microsoft Academic, pode-se observar que o tema cresce constantemente. No ano de 2020, houve 399 publicações e mais de 10 mil citações sobre o tema. A pesquisa foi realizada no dia 03 de junho de 2021. Apesar do aumento na quantidade de artigos publicados, modelagem de ameaça é um assunto que poderia ser mais bem explorado pelas empresas e pela academia. O artigo realiza uma análise textual utilizando como base, a publicação do Shostack (2014), considerado como referência no assunto de modelagem de ameaça, posteriormente realizou-se uma análise bibliométrica utilizando as palavras com maior reincidência do respectivo livro. Com base nos artigos encontrados, realizou-se uma verificação sobre os temas abordados pelos artigos, para encontrar os modos de como o tema de modelagem de ameaça é abordado, suas técnicas utilizadas e de que modo é empregado. Este artigo tem como contribuição identificar as técnicas utilizadas para mapeamento de ameaça na literatura, assim como suas aplicações, com a proposição de que, pelo fato de ter sido uma das primeiras técnicas aceitas pela comunidade, STRIDE pode ser a técnica predominante dentro da literatura entre as outras existentes. Relacionar as técnicas existentes na literatura e apresentar qual técnica de modelagem de ameaça mais abordada entre os artigos analisados. O artigo está estruturado da seguinte forma: seção 2 traz a fundamentação teórica sobre o tema modelagem de ameaça com uma breve introdução sobre gestão e avaliação de risco, a seção 3 explica a metodologia utilizada para execução da análise textual e realização da bibliometria, seção 4 analisa os resultados encontrados nos artigos da bibliometria e evidencia o método mais utilizado pelos artigos analisados e finalmente, a seção 5 traz a conclusão e considerações finais sobre o artigo.

Fundamentação Teórica: A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa, guardada para uso restrito ou exposta ao público para consulta ou aquisição

(DOS REIS, 2011). Em uma visão geral, a segurança da informação é constituída por três princípios fundamentais: confidencialidade, integridade e disponibilidade (ABNT ISO/IEC 27001, 2013) que podem ser definidos como:

- **Confidencialidade:** visa garantir que a informação não seja acessível a indivíduos, entidades ou processos não autorizados. A confidencialidade deve ser preservada para cada unidade de dados e deve ser mantida enquanto os dados estão armazenados em um sistema, quando são transmitidos e quando chegam ao seu destinatário.
- **Integridade:** integridade se refere a consistência do estado da informação.Toda e qualquer modificação não autorizada dos dados, seja ela intencional ou não, é considerada uma violação deste princípio.
- **Disponibilidade:** visa garantir que a informação esteja disponível para uso legitimo quando necessário, para os usuários com acessos autorizados.

Gestão de risco cibernético é o processo de identificação, análise, avaliação e abordagem das ameaças à segurança cibernética de uma organização. Uma abordagem sistemática de gestão de riscos de segurança da informação é necessária para se identificar as necessidades da organização em relação aos requisitos de segurança da informação e para criar um sistema de gestão de segurança da informação (SGSI) que seja eficaz (ABNT ISO 27005, 2019). Modelagem de ameaça atua diretamente no processo de avaliação de risco: na identificação, análise e avaliação dos riscos encontrados, conforme mostra a Figura 1 (ABNT ISO/IEC 27005:2019):



Fonte: ABNT ISO/IEC 27005:2019

Figura 1. Gestão de Risco conforme ABNT ISO/IEC 27005:2019

Pode-se definir modelagem de ameaças como um processo estratégico que visa considerar possíveis cenários de ataque e vulnerabilidades em um aplicativo proposto ou ambiente existente. com o objetivo de identificar claramente os níveis de risco e impacto (VÉLEZ E MORANA, 2015). STRIDE é atualmente o método de modelagem de ameaças mais maduro, desenvolvido por Loren Kohnfelder e Praerit Garg em 1999 e adotado pela Microsoft em 2002. Este método evoluiu ao longo do tempo para incluir novas tabelas específicas de ameaças e as variantes STRIDE-por-Elemento e STRIDE-por-Interação (SHEVCHENKO, 2018).

De acordo com Shostack (2014) STRIDE é um mnemônico para coisas que dão errado na segurança, significando: *Spoofing* (falsificação), *Tampering* (adulteração), *Repudiation* (repúdio), *Information Disclosure* (divulgação de informações), *Denial of Service* (negação de serviço) e *Elevation of Privilege* (elevação de privilégio). Cada letra que compõe o nome STRIDE é uma categoria. A definição de cada categoria, em português, é explicada na sequência:

- S: Falsificação é fingir ser algo ou alguém que você não é.
- T: Adulterar é modificar algo que você não deve modificar. Pode incluir pacotes na rede (com ou sem fio), *bit*s no disco ou *bit*s na memória.
- R: Repúdio significa alegar que você não fez algo (independentemente se você fez ou não).
- I: Divulgação de informações é sobre a exposição de informações a pessoas não autorizadas.
- D: Negação de serviço são ataques projetados para impedir que um sistema forneça serviço, inclusive travando-o, tornando-o excessivamente lento ou preenchendo todo o seu armazenamento.
- E: Elevação de privilégio é quando um programa ou usuário é tecnicamente capaz de fazer coisas que eles não deveriam fazer.

STRIDE analisa vulnerabilidades contra cada componente do sistema que pode ser explorado por um invasor para comprometer todo o sistema (KHAN *et al*., 2017). Com base nas 6 classificações do STRIDE, é possível então classificar as ameaças, inserindo cada ameaça encontrada em sua devida classificação no STRIDE. Após a classificação das ameaças, se faz necessário avaliar o tratamento para cada ameaça encontrada, escolhendo se a ameaça será mitigada, se a responsabilidade será transferida ou se o risco será aceito. A opção de mitigara ameaça é sempre a mais favorável, as outras opções devem ser consideradas apenas caso haja tolerância ao risco. Recomenda-se realizar uma validação após a coleta de todas as ameaças, as tarefas de validação, onde incluem verificar o modelo, verificar se procurou cada ameaça e verificar seus testes. Provavelmente, também pode validar o modelo uma segunda vez quando estiver perto de enviar ou implantar. Scandariato *et al*. (2015) em seu estudo descritivo da técnica de modelagem de ameaças da Microsoft, mostram que o método STRIDE tem uma taxa moderadamente baixa de falsos positivos e uma taxa moderadamente alta de falsos negativos. STRIDE foi aplicado com sucesso a sistemas cibernéticos e ciberfísicos (SHEVCHENKO, 2018).

METODOLOGIA

O referencial teórico permite verificar o estado do problema a ser pesquisado, sob o aspecto teórico e de outros estudos e pesquisas já realizados (MARCONI; LAKATOS, 2003). Olivro que pode ser considerado como referência sobre modelagem de ameaça, tem sido de Adam Shostack, "*Threat Modeling Designing for Security*", lançado no ano de 2014. O livro possuía 704 citações, na data de pesquisa da bibliometria, na data de 03/06/2021. Para a análise textual, utilizou-se o programa "Iramuteq" e o livro de Shostack como base para a pesquisa, para ser possível identificar quais as palavras mais utilizadas sobre o tema.

Este método foi escolhido para que fosse possível realizar uma bibliometria fidedigna sobre o assunto, possibilitando que seja possível encontrar palavras que são realmente relacionadas ao tema. Com base nos resultados apresentados pelo programa "Iramuteq", utilizando o próprio aplicativo, foi feito uma nuvem de palavras para fácil entendimento e tornar possível identificar quais as palavras mais citadas no livro. Com base no resultado, realizar uma bibliometria sobre o assunto. O resultado apresentou que as palavras mais utilizadas foram: *Threat, Model, System, Security, Datum e Attack,* conforme nuvem de palavras da Figura 2.

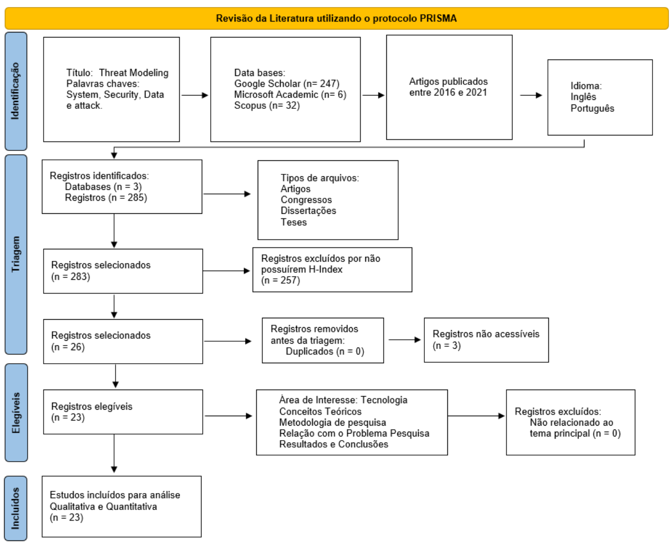
Fonte: Resultado da Pesquisa

Figura 2. Nuvem de palavras

Em posse das palavras mais utilizadas, iniciou-se a bibliometria sobre o assunto. A busca foi realizada utilizando o programa "*Publish or Perish v7*", na data de 27/08/2021, com os parâmetros apresentados na sequência:

- No título, as palavras *Threat Modeling* foram inseridas. Como palavras chaves, foram utilizadas as palavras *System, Security, Datum e Attack.* Utilizando-se *and* entre as palavras chaves.
- As databases utilizadas foram: Google Scholar, Microsoft Academic e Scopus.
- Registros publicados entre 2016 e 2021, que estivessem disponíveis no idioma inglês ou português. Totalizando 285 registros encontrados.
- Na etapa de triagem, foram selecionados artigos de congresso, dissertações ou teses. Realizando a remoção de 2 registros por serem registros de patentes, totalizando 283 registros.

Na próxima triagem, foi utilizado a medição baseada em *H-Index (H-Index, 2021)*, onde apenas documentos que são considerados relevantes e possuem certa quantidade de citações são categorizados como *H-Index*. Nesta primeira triagem, foram removidos 257 registros. Totalizando 26 registros para verificação após triagem. Não foram encontrados registros idênticos ou repetidos. Ao tentar acessar os 26 registros restantes, notou-se que 3 não estavam acessíveis, sendo removidos. Totalizando 23 registros para serem verificados. Após avaliação dos artigos, foram selecionados todos os 23 artigos para a análise quantitativa e qualitativa. Com base nessas informações, utilizou-se o protocolo PRISMA-P (Moher *et al*., 2015) para ilustrar o resultado apresentado, conforme Figura 3.



Fonte: Resultado da Pesquisa

Figura 3. Prisma-P

Com base no resultado da pesquisa bibliométrica, foi possível verificar que existem publicações de artigos considerados relevantes em função das citações ao longo dos últimos cinco anos, onde foram publicados 6 artigos e 157 citações em 2016, 5 artigos e 229 citações em 2017, 7 artigos e 221 citações em 2018, 4 artigos e 231 citações em 2019, 1 artigo e 10 citações em 2020. Não foram encontrados artigos considerados relevante, até a data da pesquisa, no ano de 2021. conforme observado na Figura 5.

Fonte: Resultado da pesquisa

Figura 4. Artigos relevantes publicados entre 2016 e 2021

Considerando os 23 artigos obtidos, foi iniciado uma verificação quantitativa e qualitativa em cada um deles. Essa verificação aborda os tipos de defesas utilizadas ou a apresentação de um novo *framework* para modelagem de ameaça. Foram considerados todos os métodos apresentados como foco do artigo, havendo artigos que utilizaram mais de um método existente no desenvolvimento, proposta de novo *framework* ou a utilização de uma modelagem existente. Não foram considerados os métodos existentes citados em trabalhos relacionados e que não foram utilizadas para o desenvolvimento do artigo. Na sequência, apresentam-se o conteúdo analítico dos 23 artigos:

1. *An agent-based approach to modeling insider threat*, (SOKOLOWSKI; BANKS; DOVER, 2016)apresentam uma nova modelagem de ameaça comportamental levando em consideração o potencial de uma ameaça interna ser desenvolvida em uma organização devido alguns atributos de sua cultura. O modelo considera todos os funcionários da organização e sua probabilidade de se tornarem uma ameaça interna.
2. *Goal Based Threat Modeling for Peer-to-Peer Cloud*, (DE; BARIK; BANERJEE, 2016) discute sobre ameaças relacionadas a redes ponto a ponto em nuvem, sem servidores centrais. Os autores propõem uma reclassificação dos ataques com base nos objetivos dos atacantes, propondo uma modelagem de ameaça com foco no atacante.
3. *pwnpr3d: an attack-graph-driven probabilistic threat-modeling approach,* (JOHNSON *et al*., 2016) apresentam uma abordagem probabilística de modelagem de ameaças para geração automática de gráficos de ataque baseado em modelagem de rede. O objetivo é fornecer às partes interessadas em organizações com uma abordagem holística que fornece visão geral de alto nível e detalhes técnicos. PwnPr3d permite automaticamente identificar e quantificar um amplo conjunto de ameaças, cobrindo a maior parte da classificação STRIDE. Como resultado principal, pwnpr3d identifica e quantifica automaticamente um amplo conjunto de ameaças como: falsificação de identidade, adulteração de dados, divulgação de informações, negação de serviço e escalonamento de privilégios.
4. *Software and attack centric integrated threat modeling for quantitative risk assessment,* (POTTEIGER; MARTINS; KOUTSOUKOS, 2016) apresenta uma abordagem quantitativa e integrada em modelagem de ameaça que combina abordagem centralizadas em software e em técnicas de ataque. Integrando a ameaça centrada no software e a ameaça centrada no ataque, especialistas em segurança são capazes de analisar risco de

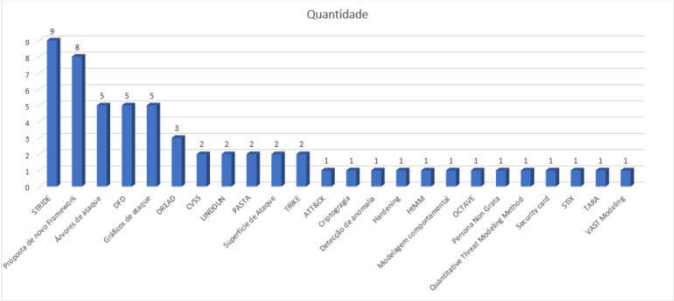
vulnerabilidade, bem como caminhos específicos que podem ser comprometidos. Atribuindo um valor de risco a cada atributo em um componente de arvore de ataque, torna-se possível uma análise quantitativa padronizada de um componente de sistema.

5. *Threat modeling for automotive security analysis* (MA; SCHMITTNER, 2016) Comentam como conduzir modelagem de ameaças para análise de segurança automotiva durante o ciclo de vida de desenvolvimento. Propõe uma abordagem prática e eficiente para a modelagem de ameaças, estendendo o suporte a ferramentas existentes e demonstrando sua aplicabilidade e viabilidade, utilizando Diagrama de Fluxo de Dados e STRIDE. Com base no DFD, é possível identificar ameaças originadas de fluxos de dados usando uma metodologia de identificação de ameaças, e com o STRIDE, avaliar a gravidade das ameaças. Os autores demonstram que a modelagem de ameaças, usando ferramentas existentes, pode ser um método de análise útil e eficiente para segurança automotiva em diferentes fases do ciclo de vida de desenvolvimento automotivo.
6. *Threat modeling for cloud data center infrastructures* (Alhebaishi *et al*., 2016) aplica exercícios de modelagem de ameaça com base em duas infraestruturas em nuvens representativas usando vários métodos populares de modelagem de ameaças, incluindo: superfície de ataque, árvores de ataque, gráficos de ataque e métricas de segurança com base em árvores de ataque e gráficos de ataque. Este trabalho pode beneficiar os provedores de nuvem ao demonstrar como os modelos de ameaças e métricas podem ajudá-los a avaliar e melhorar a segurança de suas nuvens.
7. *Adapting threat modeling methods for the automotive industry* (KARAHASANOVIC; KLEBERGER; ALMGREN, 2017) demonstra como o processo de modelagem de ameaça, comum para a indústria de computadores, pode ser adaptado e aplicado na indústria automotiva. A contribuição geral é obtida fornecendo dois métodos de modelagem de ameaças que são especificamente adaptados para o conceito de carro conectado e podem ser usados posteriormente por especialistas automotivos. O primeiro método, TARA, representa uma abordagem centrada no invasor, enquanto o segundo método, STRIDE, investiga a arquitetura de software do sistema e pertence à abordagem centrada no software. As bibliotecas criadas pelo método TARA e o modelo usado pelo método STRIDE são um bom ponto de partida para qualquer aplicação futura. A pesquisa descrita neste artigo, incluindo a validação real dos resultados do STRIDE em hardware real, demonstra a utilidade desses métodos permitindo que especialistas sejam capazes de incluí-lo em seu conjunto de ferramentas para análises futuras.
8. *Attack-Graph Threat Modeling Assessment of Ambulatory Medical Devices*(LUCKETT; MCDONALD; GLISSON, 2017) apresenta modelagem de gráfico de ataque como uma solução viável para identificar vulnerabilidades, avaliação de risco e formação de mitigação estratégias para defender dispositivos médicos ambulatoriais de atacantes. Esta pesquisa destaca a necessidade de modelagem em dispositivos ambulatoriais separadamente dos dispositivos médicos tradicionais por demonstrando certos vetores de ataque que representam maior risco para dispositivo ambulatoriais, como ataques físicos e engenharia social. Trabalhos futuros irão considerar a arquitetura do gráfico de ataque.
9. *Modeling And Analysis Of Identity Threat Behaviors Through Text Mining Of Identity Theft Stories* (NOKHBEH ZAEEM *et al*., 2017) Possui o objetivo de analisar os dados de roubo de identidade, esta pesquisa propõe uma abordagem que envolve a coleção inédita de notícias online e reportagens sobre o tema roubo de identidade. Utilizando técnicas de mineração de texto, este artigo apresenta uma análise estatística de padrões de comportamento e recursos usados por ladrões e fraudadores para cometer roubo de identidade, incluindo os atributos de identidade comumente vinculados a crimes de identidade, recursos que os ladrões empregam para conduzir crimes de identidade e padrões temporais de comportamento criminoso. O algoritmo de Avaliação e Predição de Ameaças de Identidade (ITAP) proposto no artigo foi projetado de maneira linear, em que cada etapa pode ser realizada separadamente e integrada para construir todo o mecanismo analítico.
10. *threat modeling and mitigation of medical cyber-physical systems* (Almohri *et al*., 2017) foca a investigação em um entendimento completo da modelagem de ameaças em Sistemas médicos cibernéticos físicos (MCPS). MCPS visam melhorar a eficácia do tratamento do paciente, fornecer informações inteligentes para o cuidador e garantir a segurança do paciente. Por meio do esboço de uma arquitetura abstrata de um MCPS, foram examinadas as funções dos componentes e das partes interessadas, demonstrando várias opções de modelagem de ameaças no MCPS, como criptografia, *hardening* e detecção de anomalia.
11. *STRIDE-based threat modeling for cyber-physical systems* (khan *et al*., 2017) apresenta uma estrutura de modelagem de ameaças abrangente para CPS usando STRIDE, uma abordagem sistemática para garantir a segurança do sistema no nível do componente, concebe uma metodologia viável e eficaz para aplicar STRIDE e, em seguida, a demonstra em testes de laboratório baseado em ambientes reais. O artigo identificou o STRIDE como uma abordagem eficaz para garantir a segurança do sistema no nível do componente. Ao identificar vulnerabilidades em nível de componente e suas possíveis consequências físicas, o STRIDE pode lidar com esses desafios de maneira eficaz.
12. *A meta language for threat modeling and attack simulations*(JOHNSON; LAGERSTRÖM; EKSTEDT, 2018) apresenta ataque de Metalinguagem (MAL), que pode ser usada para projetar linguagens de ataque específicas de domínio. O MAL fornece um formalismo que permite a geração semiautomática, bem como o cálculo eficiente de gráficos de ataque grandes. O MAL permite que especialistas em segurança codifiquem o conhecimento específico do domínio para permitir simulações de ataques a sistemas no domínio de interesse. As linguagens de modelagem de ataque específicas de domínio assim geradas podem ser posteriormente usadas e reutilizadas por pessoas com menos experiência em segurança, a fim de avaliar automaticamente a segurança de sistemas específicos dentro do domínio.
13. *A threat modeling approach for cloud storage brokerage and file sharing systems* (TORKURA *ET AL*., 2018) apresenta um esquema de modelagem de ameaças para analisar e identificar ameaças e riscos em sistemas de corretagem em nuvem. Com base em árvores de ataque, gráficos de ataque e diagramas de fluxo de dados que representam as interconexões entre os riscos de segurança existentes. A abordagem do artigo é adequada para melhorar a avaliação de risco de segurança para serviços em nuvem em geral. Provedores de nuvens também podem usar a proposta para fornecer melhores métricas de segurança.
14. *Cyber threat modeling: Survey, assessment, and representative framework* (BODEAU; MCCOLLUM; FOX, 2018) Este relatório fornece uma pesquisa de estruturas de modelagem de ameaças cibernéticas, apresenta uma avaliação comparativa das estruturas pesquisadas e estende uma estrutura existente para servir de base para a modelagem de ameaças cibernéticas para uma variedade de finalidades. A estrutura inicial e o modelo apresentado neste relatório podem servir como um recurso para outros setores de infraestrutura crítica. Mesmo as organizações no setor financeiro dependem ou dependerão cada vez mais de sistemas cibe físicos (por exemplo, caixas eletrônicos) e tecnologia operacional. Portanto, a modelagem de ameaças cibernéticas para sistemas físicos cibernéticos, tecnologia operacional e a Internet das coisas é uma área de trabalho futuro.
15. *Solution-aware data flow diagrams for security threat modeling*(SION *et al*., 2018) enriquece os diagramas de fluxo de dados com elementos de solução de segurança, que são levados em consideração durante a modelagem de ameaças. A abordagem de modelagem é apoiada por uma implementação de prova de conceito de uma estrutura de modelagem de ameaças e validada no contexto de uma análise STRIDE de uma solução de videoconferência industrial baseada em WebRTC. Os DFD enriquecidos apresentados são peças-chave para esforços futuros

em direção a processos dinâmicos e contínuos em modelagem de ameaças.

16. *The battle for new york: a case study of applied digital threat modeling at the enterprise level*(STEVENS *et al*., 2018) , neste estudo de caso, os autores apresentam uma nova modelagem de ameaças, o Centro de gravidade (CoG) ao New York *CityCyber Command*: a principal organização de defesa digital da cidade mais populosa dos Estados Unidos. Descobriu-se que a modelagem de ameaças melhorou a autoeficácia; 20 de 25 participantes o incorporaram regularmente em suas tarefas diárias 30 dias após o treinamento, sem aviso prévio. Após 120 dias, as estratégias de mitigação de ameaças projetadas pelo participante forneceram benefícios de segurança tangíveis para NYC, incluindo o bloqueio de 541 tentativas de intrusão exclusivas, evitando o sequestro de cinco contas de usuário com privilégios e abordando três vulnerabilidades de servidor voltadas para o público. No geral, esses resultados sugerem que a introdução da modelagem de ameaças pode fornecer benefícios valiosos em um ambiente corporativo.
17. *Threat modeling for mobile health systems* (CAGNAZZO *et al*., 2018) enfoca os desafios de segurança e oferece uma solução de mitigação, especialmente com foco na autenticação e criptografia para dispositivos com recursos limitados. Ele identifica ativos em um protótipo de ecossistema mHealth e classifica ameaças com a metodologia STRIDE. Além disso, o documento identifica os níveis de risco associados usando DREAD e descreve possíveis estratégias de mitigação para fornecer um ambiente razoável e confiável. Pesquisas futuras validarão a abordagem por meio da implementação em um cenário do mundo real, para obter mais *insights*. Outro desafio no ecossistema mHealth é como os dispositivos de substituição, ou dispositivos que têm uma grande flutuação, são tratados.
18. *Threat modeling: a summary of available methods* (SHEVCHENKO *et al*., 2018) apresenta doze métodos de modelagem de ameaças de uma variedade de fontes e visam diferentes partes do processo de modelagem de ameaça. Os autores fazem uma breve descrição de métodos conhecidos, como STRIDE e arvores de ataque, assim como métodos ainda não citados neste artigo, como TRIKE e OCTAVE. Nenhum método de modelagem de ameaça é recomendado em vez de outro; a decisão de qual(is) método(s) usar deve ser baseada nas necessidades do projeto e suas preocupações específicas.
19. *Cyber security threat modeling for supply chain organizational environments*(YEBOAH-OFORI; ISLAM, 2019) possui o objetivo de investigar e compreender as ameaças da Cadeia de Suprimentos Cibernético (CSC). Em particular, o documento contribui para modelar e analisar ataques de CSC e relatórios de ameaças cibernéticas entre as partes interessadas da CSC. Considerando conceitos relevantes baseados no modelo ATT&CK: objetivo, ator, ataque, TTP e ator de ameaça para a cadeia de suprimentos, modelo de ameaça e domínio de requisitos, modelando o ataque usando o modelo de ameaça STIX. O estudo mostrou que o objetivo do adversário é penetrar nas cadeias de abastecimento de entrada e saída e manipular dados. Estudos adicionais são necessários para modelar ameaças à segurança de CSC de sistemas de subestação de rede elétrica e de diferentes cenários de ataque. Também pode se determinar os riscos de crimes cibernéticos em sistemas físicos cibernéticos.
20. *Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures* (HOMOLIAK *et al*., 2019) propõe uma taxonomia estrutural e uma nova categorização de pesquisas que contribuem para a organização e desambiguação de incidentes de ameaças internas e as soluções de defesa usadas contra eles. O objetivo da categorização é sistematizar o conhecimento na pesquisa de ameaças internas ao mesmo tempo em que usa um método de teoria fundamentada existente para uma revisão rigorosa da literatura. O estudo identificou quatro categorias principais de esforços de pesquisa e desenvolvimento: categoria de incidentes e conjuntos de dados, categoria de análise de incidentes, categoria simulações e categoria de soluções de defesa.
21. *Threat modeling–A systematic literature review*(XIONG; LAGERSTRÖM, 2019) apresenta uma revisão da modelagem de ameaças com base em consultas sistemáticas em quatro bancos de dados científicos: IEEE Xplore, Scopus, Springer link e Web of Science. Evidenciando os métodos encontrados: STRIDE, arvore de ataque, DREAD entre outros, classificando as modelagens de ameaças encontradas entre automática, manual, formal e gráfica. Como trabalho futuro, os autores propõem um método de modelagem automática de ameaças, baseado na Meta Attack Language (MAL), validá-lo em estudo de caso com testes de laboratórios em ambientes baseados em mundo real.
22. *Toward the automation of threat modeling and risk assessment in IoT* systems (CASOLA *et al*., 2019) propõe uma abordagem que visa apoiar a análise de segurança de um sistema *IoT* por meio de um processo quase totalmente automatizado de modelagem de ameaças e avaliação de riscos, utilizando STRIDE, o que também ajuda a identificar os controles de segurança a implementar a fim de mitigar os riscos de segurança existentes. Como direção futura, planejam estender o processo integrando recursos de avaliação de segurança automatizada, a fim de permitir a análise do nível de segurança fornecido por diferentes implantações em tempo de design e pretendem integrar recursos de testes de penetração automatizados no processo.
23. *Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics*(ZIMBA *et al*., 2020) Para superar as limitações atuais da dinâmica de rede de ataque enfrentada nos estudos de APT, um modelo inovador de detecção de ataque de APT baseado em uma abordagem de aprendizado semi supervisionado com características de redes complexas é proposto. Toda a rede alvo é modelada como uma pequena rede, e a rede APT-Attack Network (APT-AN) evolui como uma rede sem escala. Esse modelo é útil para analistas de segurança e rede como um suplemento ao IDS automatizado, uma vez que alguns aspectos do ciclo de ataque do APT não podem ser detectados automaticamente. Um dos desafios notáveis do modelo proposto é a alta sobrecarga computacional.

A Figura 6 mostra um resumo sobre os métodos apresentados: Com base na quantidade de citações sobre o método apresentado, pode-se criar um histograma, evidenciando a quantidade de vezes que a solução foi utilizada, conforme Figura 7.



Fonte: Resultado da pesquisa

Figura 7. Quantidade de utilização de cada método nos artigos

ANÁLISE DE RESULTADOS

Com base nos artigos analisados, foram encontrados 24 métodos que podem ser utilizados para modelagem de ameaça e 8 propostas de novos métodos ou *frameworks*. Observando que existe uma grande variedade disponível que são considerados métodos para aplicação de modelagem de ameaça, foi possível confirmar que STRIDE é o método mais utilizado, nos últimos 5 anos, para aplicação de modelagem de ameaça. Os resultados da abordagem STRIDE são mais significativos, facilmente compreensíveis e abrangentes o suficiente para os projetistas de sistemas desenvolverem soluções de segurança apropriadas. O resultado do STRIDE pode alimentar os processos de análise de risco para estabelecer as ameaças mais

críticas e, além disso, o desenvolvimento das medidas de mitigação mais adequadas que devem ser aplicadas. Há a possibilidade de utilizar mais de um método ao mesmo tempo, aumentando a eficiência na aplicação do método de modelagem de ameaça. Essa ação é indicada quando se nota a possibilidade de melhoria no resultado ao se utilizar mais de um método ou quando apenas um método não retornará o resultado esperado. Nota-se que nenhum método é considerado perfeito, soberano, a prova de falhas ou mais indicado entre os métodos existentes. A escolha do método que será utilizado dependerá da necessidade do projeto, seus objetivos, preocupações especificas e o conhecimento do profissional que aplicará a modelagem de ameaça utilizando o método escolhido. Pode-se notar a necessidade de mais testes empíricos relacionados a aplicação de modelagem de ameaça. Entre os 23artigos, apenas 3 artigos confirmam a realização de testes empíricos, que estão numerados como: 7, 16 e 19. Com base nas buscas realizadas e resultados encontrados, nota-se que a modelagem de ameaça é proposta na mitigação de riscos, colaborando para a gestão de riscos existentes. Sua implementação é recomendada para encontrar ameaças ainda não mapeadas: seja no desenvolvimento do software, alteração do ambiente ou inclusão de um novo recurso. É possível identificar que existem artigos relacionados a modelagem de ameaça comportamental, mas não há exemplos empíricos sobre a utilização da técnica ou trabalho conjunto com outros setores para uma avaliação real. Com base nas aplicações apresentadas, nota-se que há uma grande variedade de áreas que podem ser beneficiadas com a implementação da prática de modelagem de ameaça. Os artigos citam exemplos onde a modelagem de ameaça pode ser empregada para melhorar a segurança utilizando diversos tipos diferentes de tecnologias e com diferentes tipos de fundamento.

CONSIDERAÇÕES FINAIS

O artigo realizou uma análise textual utilizando como base, a publicação do autor Shostack, considerado como referência no assunto de modelagem de ameaça, posteriormente foi feito uma análise bibliométrica em três *databases* disponíveis gratuitamente utilizando as palavras encontradas. Com base nos artigos encontrados, foi realizado uma verificação dos artigos para encontrar o modo como o tema modelagem de ameaça é abordado, técnicas utilizadas e de que modo é empregado. Como limitação, a busca poderia ser realizada também em outras *databases*, que os autores não possuem acesso no momento. Este artigo teve como contribuição a identificação das diversas técnicas utilizadas para mapeamento de ameaça na literatura, confirmando a proposição de que STRIDE é a técnica predominante utilizada na literatura entre as outras evidenciadas nos artigos encontrados. Nota-se que a modelagem de ameaça pode ser utilizada de maneiras diferentes, em assuntos diversos e em qualquer etapa no desenvolvimento de um software, projeto ou na melhoria da segurança de um ambiente. Também pode influenciar a adoção, criação ou alteração de processos existentes. O tema está em ascensão no ambiente acadêmico e pode ser utilizado também em ambientes corporativos, apesar de haver poucos estudos empíricos. Nos artigos avaliados, pode-se observar a falta de artigos com estudos empíricos, que podem auxiliar na avaliação da utilização da ferramenta em mundo real e seu real benefício. Modelagem de ameaça é um tema relevante para a proteção adequado do meio empresarial e faz-se necessário para obter um ambiente cada vez mais seguro. Como trabalhos futuros, pode-se aplicar modelagem de ameaça com foco em ambientes e aplicações em computadores. Não foram encontrados nos artigos a utilização de modelagem de ameaça com foco em computadores utilizados por este público, visando mitigação de riscos relacionados a vazamento de dados e informações com foco nesta origem, apesar do aumento da quantidade de pessoas que utilizam microcomputadores empresariais em sua residência.

REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2013 Disponível em: https://www.abntcatalogo.com.br/norma.aspx?Q=DCB58239A687C830CA01C1F90723A6553E174C26F25FA42B6F9DE1045E9C9F31 Acesso em: 01/09/2021

ABNT NBR ISO/IEC 27005:2019 Disponível em: https://www.abntcatalogo.com.br/norma.aspx?Q=20C1ADCBBAE79428CA01C1F90723A6556C572963BEFAF2E3FBABFD6FE89F1B11 Acesso em: 01/09/2021

ALHEBAISHI, Nawaf *et al*. Threat modeling for cloud data center infrastructures. In: International Symposium on Foundations and Practice of Security. Springer, Cham, 2016. p. 302-319.

ALMOHRI, Hussain *et al*. On threat modeling and mitigation of medical cyber-physical systems. In: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). IEEE, 2017. p. 114-119.Bodeau, D. J.; McCollum, C. D.; Fox, D. B. Cyber threat modeling: Survey, assessment, and representative framework. MITRE CORP MCLEAN VA MCLEAN, 2018.

CAGNAZZO, Matteo *et al*. Threat modeling for mobile health systems. In: 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). IEEE, 2018. p. 314-319.

CASOLA, Valentina *et al*. Toward the automation of threat modeling and risk assessment in IoT systems. Internet of Things, v. 7, p. 100056, 2019.

DE, Sanghamitra; BARIK, Mridul Sankar; BANERJEE, Indrajit. Goal based threat modeling for peer-to-peer cloud. Procedia Computer Science, v. 89, p. 64-72, 2016.

HOMOLIAK, Ivan *et al*. Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR), v. 52, n. 2, p. 1-40, 2019.

JOHNSON, Pontus *et al*. pwnpr3d: an attack-graph-driven probabilistic threat-modeling approach. In: 2016 11th International Conference on Availability, Reliability and Security (ARES). IEEE, 2016. p. 278-283.

JOHNSON, Pontus; LAGERSTRÖM, Robert; EKSTEDT, Mathias. A meta language for threat modeling and attack simulations. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. 2018. p. 1-8.

KARAHASANOVIC, Adi; KLEBERGER, Pierre; ALMGREN, Magnus. Adapting threat modeling methods for the automotive industry. In: Proceedings of the 15th ESCAR Conference. 2017. p. 1-10.

KHAN, Rafiullah *et al*. STRIDE-based threat modeling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, 2017. p. 1-6.

LUCKETT, Patrick; MCDONALD, J. Todd; GLISSON, William Bradley. Attack-graph threat modeling assessment of ambulatory medical devices. arXiv preprint arXiv:1709.05026, 2017.

MA, Zhendong; SCHMITTNER, Christoph. Threat modeling for automotive security analysis. Advanced Science and Technology Letters, v. 139, p. 333-339, 2016.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de metodologia científica. 5. ed.-São Paulo: Atlas, 2003. Microsoft Academic https://academic.microsoft.com/topic/140547941/publication/search?q=Threat%20model&qe=And(Composite(F.FId%253D140547941)%252CTy%253D%270%27)&f=&orderBy=0 Acesso em: 01/09/2021

MOHER, D., *et al*. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement, https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/2046-4053-4-1. Acesso em: 01/09/2021.

POTTEIGER, Bradley; MARTINS, Goncalo; KOUTSOUKOS, Xenofon. Software and attack centric integrated threat modeling for quantitative risk assessment. In: Proceedings of the Symposium and Bootcamp on the Science of Security. 2016. p. 99-108.

REIS, Hugo Toffalini Esteves dos. Segurança da informação e a Educação a distância. In: Anais do Congresso Nacional Universidade, EAD e Software Livre.

SCANDARIATO, Riccardo; WUYTS, Kim; JOOSEN, Wouter. A descriptive study of Microsoft's threat modeling technique. Requirements Engineering, v. 20, n. 2, p. 163-180, 2015.

SHEVCHENKO, Nataliya *et al*. Threat modeling: a summary of available methods. Carnegie Mellon University Software Engineering Institute Pittsburgh United States, 2018.

SHOSTACK, Adam. Threat Modeling Designing for Security P.25, Editora WILEY, 2014.

SION, Laurens *et al*. Solution-aware data flow diagrams for security threat modeling. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing. 2018. p. 1425-1432.

SOKOLOWSKI, John A.; BANKS, Catherine M.; DOVER, Thomas J. An agent-based approach to modeling insider threat. Computational and Mathematical Organization Theory, v. 22, n. 3, p. 273-287, 2016.

STEVENS, Rock *et al*. The battle for new york: a case study of applied digital threat modeling at the enterprise level. In: 27th {USENIX} Security Symposium ({USENIX} Security 18). 2018. p. 621-637.

Threat model - Microsoft Academic. Disponível em: https://academic.microsoft.com/topic/140547941/publication/search?q=Threat%20model&qe=And(Composite(F.FId%253D140547941)%252CTy%253D%270%27)&f=&orderBy=0 Acesso em: 01/09/2021

TORKURA, Kennedy A. *et al*. A threat modeling approach for cloud storage brokerage and file sharing systems. In: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2018. p. 1-5.

UCEDAVELEZ, Tony; MORANA, Marco M. Risk Centric Threat Modeling: process for attack simulation and threat analysis. John Wiley & Sons, 2015.

XIONG, Wenjun; LAGERSTRÖM, Robert. Threat modeling–A systematic literature review. Computers & security, v. 84, p. 53-69, 2019.

YEBOAH-OFORI, Abel; ISLAM, Shareeful. Cyber security threat modeling for supply chain organizational environments. Future Internet, v. 11, n. 3, p. 63, 2019.

ZAEEM, Razieh Nokhbeh *et al*. Modeling and analysis of identity threat behaviors through text mining of identity theft stories. Computers & Security, v. 65, p. 50-63, 2017.

ZIMBA, Aaron. *et al*. Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics. Future Generation Computer Systems, v. 106, p. 501–517, 2020.

****