MAV: Metodologia de Análise de Ameaças e Vulnerabilidades em um framework integrado multiplataforma

Ariel M. Silva[1], João Pedro Pereira[1], Raissa S de Moura[1], Sérgio Ribeiro[1]

[1]CPQD - Centro de Pesquisa e Desenvolvimento em Telecomunicações
R. Dr. Ricardo Benetton Martins, 1000 – Campinas – SP – Brazil

{ariels,joaolc,raissak,sribeiro}@cpqd.com.br

Abstract. *This paper proposes a threat and vulnerability analysis methodology characterized by a high number of interconnected components. The methodology is part of an integrated multiplatform security assessment framework and aims to identify vulnerabilities, the methods used to exploit them, the threat agents, and the threat scenarios resulting from the exploitation of the vulnerabilities. Thus, the methodology results in a list of security threat scenarios that identify the system's security flaws before they can be exploited.*

Resumo. *Este artigo propõe uma metodologia de análise de ameaças e vulnerabilidades, caracterizada por um alto número de componentes interconectados. A metodologia faz parte de um framework integrado de avaliação de segurança multiplataforma e tem como objetivo a identificação das vulnerabilidades, os métodos utilizados para explorá-las, os agentes de ameaça e os cenários de ameaça resultantes da exploração das vulnerabilidades. Assim, a metodologia resulta em uma lista de cenários de ameaças à segurança que identificam as falhas de segurança do sistema antes que possam ser exploradas.*

1. Introdução

A era digital gera um novo cenário no qual emergem novas ameaças. Uma das ameaças mais relevantes na era digital são os ciberataques. Esses ataques têm o objetivo de acessar, bloquear, modificar e corromper dados ou serviços explorando fraquezas de segurança nos ativos da organização. Segundo um estudo da Check Point, os ciberataques globais aumentaram 28% no primeiro trimestre de 2024 em comparação com o mesmo período em 2023, atingindo um número médio de 1308 ataques semanais por organização [Check Point 2024].

É indispensável que as organizações gerenciem os riscos de cibersegurança que afetam sua operação, tornando-se até mesmo um requisito legal e de mercado. De acordo com a ISO 27005 [ISO/IEC 27005 2022]. Na etapa de identificação de risco, segundo a norma, os cenários de ameaça são determinantes para tratar eficazmente os riscos de cibersegurança mais prioritários. Com o avanço crescente, as novas tecnologias requerem novos métodos a serem utilizados em projetos para enfrentar os novos desafios gerados. Métodos tradicionais de identificação de riscos de cibersegurança que subdividem o sistema em partes podem não identificar cenários de ameaça relevantes para sistemas complexos com inúmeras interconexões.

Este trabalho propõe uma metodologia para definir cenários de ameaças à segurança para sistemas digitais heterogêneos interconectados, que são sistemas onde existem diversas conexões com ativos de diferentes funções, importância, tipo e

tecnologia. Um exemplo seriam os sistemas heterogêneos IoT [GEORGIOS 2024], que integram tecnologias e ativos já utilizados na indústria com um sistema digital de controle e dispositivos IoT. No caso deste trabalho, a metodologia não se limita apenas a IoT, mas todo o sistema interconectado composto por diferentes tecnologias.

2. Análise de Ameaças Cibernéticas

Segundo o National Institute of Standards and Technology (NIST) a análise de ameaças pode ser definida como *"um processo que avalia formalmente o grau de ameaça a um sistema de informação ou empresa e descreve sua natureza."* [NIST 2012]. De maneira mais detalhada, essa avaliação permite comunicar e entender o contexto de uma aplicação, identificando possíveis atividades maliciosas. Elaborada em uma representação estruturada, a análise de ameaças pode ser aplicada em sistemas distribuídos, softwares, redes e até mesmo em planos de negócios, com o objetivo de melhorar a segurança dos ativos por meio da mitigação de potenciais incidentes [OWASP 2024].

Para a realização do mapeamento de ameaças e vulnerabilidades, é possível encontrar como mapear as ameaças em algumas metodologias já existentes como o TARA [MITRE, 2011]. As metodologias partem das vulnerabilidades encontradas, mapeiam as ameaças e controles necessários, mas sem considerar todos os cenários possíveis dentro do fluxo de dados da aplicação ou todos os cenários além das vulnerabilidades já encontradas, como por exemplo as vulnerabilidade de dia zero.

3. Metodologia Proposta

As vulnerabilidades e os métodos utilizados por atacantes mudam ao longo do tempo, um exemplo é o aparecimento de vulnerabilidades explorando falha humana e as vulnerabilidade de dia zero [ASLAN 2023]. Assim, é necessário que ao mapear as ameaças sejam identificadas as ameaças provenientes a esses cenários, ou seja, é necessário a identificação da ocorrência da ameaça em caso do surgimento de determinada vulnerabilidade.

Diante do cenário em que diversas normas e processos citam o mapeamento de ameaças como parte essencial da análise de riscos, torna-se valioso o desenvolvimento de uma metodologia que seja aplicável a diversos cenários. Por esse motivo, é proposto no escopo do projeto TecSeg [ALMEIDA 2022] um framework integrado de avaliação de segurança multiplataforma [CASSIANO 2022], que inclui a metodologia proposta de mapeamento de ameaças e vulnerabilidades.

A metodologia em conjunto com o framework permite uma automatização e atualização em "tempo real", conforme os surgimento de novas vulnerabilidades, apresentando o mapeamento das ameaças. Assim, com o diferencial de apresentar todos esses cenários para se proteger de maneira antecedente.

Por isso, é proposta uma abordagem que mapeia todos os cenários de falha e as ameaças causadores, permitindo uma abordagem que não se prenda as vulnerabilidades conhecidas mas as possibilidades de falhas do sistema, buscando um mapeamento completo baseado no fluxo de funcionamento do sistema. Este tipo de abordagem pode ser observada em análises de ameaças específicas para alguns cenários, como no caso de sistemas IoT [NAKAMURA 2019]. A metodologia proposta para atender os requisitos desejados é composta por quatro fases sequenciais:

3.1. Fase 1: Identificação da Condição Final de Ameaça

A Condição de Ameaça Final representa o estado que pode resultar em efeitos indesejados no ativo a ser protegido, sendo crucial entender essas condições e avaliar os impactos potenciais de uma ameaça. Portanto, nesta fase, propõe-se a identificação das condições finais de ameaça.

Dentro do Framework o qual a MAV está integrada, todas as entradas são fornecidas pela metodologia de contexto do Framework [BARBOSA 2024], o que permite padronizar e tornar eficiente o levantamento de dados para a aplicação da metodologia. Vale ressaltar que a MAV pode ser aplicada de forma independente do Framework em situações em que todo o contexto já foi previamente mapeado.

O primeiro passo nesta fase é identificar as variáveis de contexto, que representam características ou delimitam critérios que influenciam diretamente os estados assumidos por um sistema. Após a identificação das variáveis de contexto, é possível mapear a Condição de Ameaça Final, a qual consiste em listar todas as condições que podem ocorrer no sistema em caso da ocorrência das ameaças, resultando em um dos estados previamente mapeados.

3.2. Fase 2: Identificação de Ameaças

De acordo com o NIST [SOUPPAYA 2021], uma ameaça representa o potencial de uma fonte de ameaça explorar com sucesso uma vulnerabilidade específica do sistema de informação. Nesta fase, o objetivo é identificar as ameaças que podem afetar um sistema. Para cada condição final de ameaça mapeada na fase anterior, são identificadas as ameaças que podem levar a essa condição, bem como os ativos que seriam impactados pela ameaça. Como etapa final desta fase, cada ameaça é classificada de acordo com um modelo específico, como o modelo STRIDE [MICROSOFT 2009].

3.3. Fase 3: Identificação do Agente de Ameaças

O objetivo desta fase é identificar os agentes que podem explorar uma vulnerabilidade, consultando fontes de dados para obter informações sobre as características e a motivação dos adversários que realizam ciberataques. Conhecer os atores é crucial porque permite tomar decisões mais direcionadas com base em ameaças reais, ajustando o nível de risco e as ações de forma mais eficaz.

Com base em dados de incidentes internos e em um banco de vulnerabilidades, é possível identificar os agentes de ameaça que têm executado ciberataques na área de negócios do sistema de interesse. Para finalizar esta fase, todos os atores identificados podem ser categorizados de acordo com sua natureza, como indivíduos internos, *hackers* profissionais ou amadores, criminosos cibernéticos, nações ou grupos terroristas.

Após categorizar os atores, é essencial mapear a capacidade técnica de cada grupo, determinando se são profissionais altamente habilidosos ou atacantes amadores. Em caso de infraestruturas críticas é crucial entender as táticas que podem ser empregadas para se preparar contra os ataques cibernéticos. A última etapa desta fase envolve mapear as motivações dos atacantes para realizar ataques, identificando as vantagens que procuram obter, como objetivos financeiros ou políticos.

3.4. Fase 4: Identificação das Vulnerabilidades

Na última fase, o objetivo é preencher a tabela final relacionando cada cenário de ameaça, mapeado nas fases anteriores, onde foram identificadas as ameaças. Esta fase abrangerá o mapeamento de vulnerabilidades, controles de segurança, vetor de ataque e agentes de ameaça associados a cada ameaça mapeada.

Todo produto, ativo ou sistema possui vulnerabilidades, muitas das quais são conhecidas e divulgadas. O objetivo é verificar a presença dessas vulnerabilidades no ativo avaliado, inicialmente através da verificação manual das melhores práticas de segurança recomendadas para o ativo, problemas de segurança na arquitetura de sistemas, e a existência de vulnerabilidade. As vulnerabilidades em um sistema podem ser identificadas por meio de testes de penetração, análise de código, ferramentas de varredura de vulnerabilidades ou pesquisa em bancos de dados de vulnerabilidades, como o programa Common Vulnerabilities and Exposures (CVE), que cataloga vulnerabilidades publicamente divulgadas [CVE 2024].

O próximo passo nesta fase é identificar os vetores de ataque, que são as formas pelas quais um atacante pode explorar a vulnerabilidade para realizar um ataque. Assim, nesta etapa, as vulnerabilidades e ameaças são analisadas para criar uma lista relacionando-as aos vetores de ataque.

Utilizando a saída fornecida pela Fase 3, que lista os agentes de ameaça, é necessário relacioná-la com a lista de vulnerabilidades, realizando uma análise detalhada para cada vulnerabilidade. Isso envolve mapear quais agentes de ameaça poderiam explorar cada vulnerabilidade, considerando a capacidade técnica ou histórico de uso da vulnerabilidade e o vetor de ataque identificado.

Para concluir esta fase, é necessário relacionar os controles de segurança existentes com as vulnerabilidades encontradas. O objetivo é identificar se existem controles mitigatórios para cada vulnerabilidade identificada nas fases anteriores. Isso permite verificar se os controles estão efetivamente mitigando a vulnerabilidade ou ainda se há falhas na implementação que precisam ser corrigidas.

Uma característica importante dessa fase é a integração com as diversas fontes de informação. A metodologia MAV pode ser integrada a softwares de monitoramento e análise de riscos, possibilitando um mapeamento ágil das ameaças diante do surgimento de novas vulnerabilidades.

Um dos principais objetivos de toda a metodologia é ser amplamente funcional e adaptável a fase do ciclo de vida do sistema em análise e ao tipo de ativo avaliado, seja rede, software ou hardware. A metodologia pode ser adaptada para mapear ameaças em diferentes cenários e ambientes críticos desde a concepção do sistema.

5. Caso de Teste

Para testar a metodologia dentro do seu escopo desejado, foi realizada uma aplicação em um software de gerenciamento, controle e monitoramento de dispositivos IoT. Neste teste, foi possível avaliar todas as entradas externas da metodologia, incluindo banco de vulnerabilidades, sistemas de informação de ameaças, ferramentas de análise de código e análise da arquitetura.

Identificando as variáveis do contexto dentro do sistema de caso de teste, são observados dois grandes objetivos para a segurança do sistema: Proteger a confidencialidade da operação e proteger o processo produtivo, assim, temos duas variáveis de contexto que podem afetar esses objetivos: os dados da operação e o funcionamento do processo produtivo. Com essas variáveis é possível preencher a Tabela 1 com as situações que essas variáveis são alteradas e afetam os objetivos de segurança.

Tabela 1. Variáveis de contexto

Variáveis de Contexto	Condição Final de Ameaça
Dados de Operação	Exposição de Dados Confidenciais
Processo de Funcionamento	Processo Atrasado Processo Não Executado

Com as variáveis de contexto mapeadas, para definir as condições finais de ameaça, é necessário olhar para cada operação dentro do fluxo de dados do sistema e mapear para cada estado da operação. A identificação das condições se baseia em mapear as condições que podem ocorrer com as operações e, dentro de cada uma, quais valores as variáveis de contexto podem assumir, como mostrado no caso específico de algumas condições na Tabela 2.

Tabela 2. Mapeamento das condições finais de ameaça

Operação	Condição	ID	Variável de Contexto	Condição Final de Ameaça
Enviar Comandos	A operação não é executada	CF-1	Processo não executado	O comando do Ativo Origem não chega ao ativo destino
		CF-2	Processo não executado	O comando do Ativo origem para o destino é enviado incorreto ou alterado
	A operação é executada	CF-3	Processo atrasado	O comando do Ativo Origem não chega ao ativo destino
		CF-4	Processo atrasado	O comando do Ativo origem para o destino é enviado incorreto ou alterado
		CF-5	Exposição de dados pessoais	O ativo envia o comando em texto claro

Assim, para cada condição final mapeada é necessário ter uma tabela exclusiva abrangendo todos os itens do classificador de ameaça e verificar para cada classificador quais ameaças nos ativos relacionados à operação podem gerar a condição final. Esta é preenchida ao longo das fases formando uma única tabela no final da metodologia, a qual fornecerá o mapeamento de ameaças. Neste artigo, apenas uma condição final específica foi abordada, mas durante a aplicação foram analisadas todas as condições finais mapeadas para o cenário de aplicação.

Para o mapeamento dos agentes de ameaças, levantou-se que o escopo trata-se de uma aplicação industrial de infraestrutura crítica, assim, com base em histórico de incidentes e levantamentos em fontes de informações, foram identificados dois grupos terroristas: Allanite e Dragonfly. Essa informação será utilizada no mapeamento de vulnerabilidades, analisando os ataques realizados por esses grupos e se as táticas exploradas podem se aplicar ao sistema representando uma vulnerabilidade.

Finalizando a aplicação da metodologia, foram utilizadas as fontes de informação externas previstas nas metodologias, consultando os *softwares* de varredura, verificação manual de código, arquitetura e verificação dos componentes em bancos de vulnerabilidades. Após mapear todas as vulnerabilidades, a tabela final é preenchida para cada ameaça listada, vulnerabilidade encontrada e vetor de ataque. Assim, é possível obter a Tabela 3, que apresenta os resultados da metodologia, fornecendo um mapeamento das ameaças desde a vulnerabilidade até a condição final que a ameaça gera no sistema.

Tabela 3. Mapeamento de ameaças e vulnerabilidades

CF-1: O comando do Ativo não chega no Ativo de destino							
Ativo	**STRIDE**	**ID**	**Ameaça**	**ID**	**Vulnerabilidade**	**Vetor de Ataque**	**Agente de Aemaça**
Ativo Origem	T (Adulteração)	A-1	Ativo Origem é alterado comprometendo seu funcionamento	V-2	Injeção de payload permitindo que invasores executem comandos	Injeção de inúmeros processos no ativo	Grupos Hackers mapeados (Allanite e Drangonfly)
	I (Divulgação de Informação)	A-2	Um agente interrompe o funcionamento do Ativo Origem	V-2	Injeção de payload permitindo que invasores executem comandos	Injeção de inúmeros processos no ativo	Grupos Hackers mapeados (Allanite e Drangonfly)

Para o sistema aplicado neste caso de teste, foi possível observar o funcionamento do método proposto, bem como a aplicabilidade do mapeamento de ameaças com base nas informações das fontes externas à aplicação. Observou-se um mapeamento que auxilia encontrar as vulnerabilidades no sistema e identificar os cenários que as mesmas podem causar, permitindo a aplicabilidade de uma análise de riscos com base nos cenários mapeados.

6. Considerações Finais

Diante do crescente avanço das tecnologias, fica evidente a necessidade de estruturação de produtos que sejam capazes de conter e mitigar os impactos na segurança da informação. Frente a esse desafio, a metodologia proposta dentro do framework integrado multiplataforma foi estruturada de modo a suprir as lacunas de outras metodologias existentes no mercado, considerando todos os cenários dentro do fluxo do sistema, mapeando as ameaças de todos os tipos de vulnerabilidades.

A metodologia desenvolvida tem como objetivo garantir a alta funcionalidade ao longo do ciclo de vida dos sistemas e ativos. Dessa forma, a MAV é capaz de analisar cenários de ameaças cruciais para prevenção proativa de aplicações, propondo integração com softwares de monitoramento em tempo real, recebendo as informações no momento em que elas acontecem como uma resposta ágil ao surgimento de novas ameaças e vulnerabilidades.

Por fim, outro ponto importante a destacar é a identificação da condição final de ameaça, derivada do contexto do cenário de aplicação, que permite compreender os impactos causados pelas ameaças e auxiliar no mapeamento das vulnerabilidades, possibilitando posteriormente o cálculo de riscos. Desse modo, tomamos como próximos passos o desenvolvimento de uma metodologia de análise de riscos que use como insumo os resultados gerados pela aplicação da MAV.

7. Agradecimentos

Os autores agradecem o apoio financeiro dado a este trabalho, no âmbito do Projeto TecSEG, com o apoio do Fundo de Desenvolvimento Tecnológico das Telecomunicações (Funttel) e da Finep, através do acordo 01.21.0163.00 (1196/21). Este artigo reflete apenas as opiniões dos autores, e as agências Finep e Funttel não são responsáveis por qualquer uso que possa ser feito das informações nele contidas.

Referencias

Almeida, A., Cassiano, J. and Ribeiro, S. (2022) "TecSEG Project - Research, Development and Innovation in Security Assessment Methodologies to Brazil," 2022

International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME).

Barbosa, I. and Ribeiro, S. (2024) "Brazilian Integrated Cross-platform Security Assessment Framework: Context of Cybersecurity Methodology," Proceedings of Eighth International Congress on Information and Communication Technology.

Cassiano, J., Ribeiro, S. and Almeida, A. (2022) "ICpSAF - Integrated Cross-platform Security Assessment Framework," 6th Cyber Security in Networking Conference (CSNet).

Aslan, Ömer & Aktug, Semih & Ozkan Okay, Merve & Yılmaz, Abdullah & Akin, Erdal. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics. 12. 1-42. 10.3390/electronics12061333.

Check Point. (2024). “Shifting Attack Landscapes and Sectors in Q1 2024 with a 28% increase in cyber attacks globally”. Disponível em: https://blog.checkpoint.com/research/shifting-attack-landscapes-and-sectors-in-q1-2024-with-a-28-increase-in-cyber-attacks-globally/.

CVE (2024), "Overview”. Disponível em: <https://www.cve.org/About/Overview>. Acesso em agosto de 2022.

Georgios, Bouloukakis., Nikolaos, Georgantas., Ajay, Kattepur., Houssam, Hajj, Hassan., Valérie, Issarny. (2024). “Automating the Evaluation of Interoperability Effectiveness in Heterogeneous IoT Systems”. doi: 10.1109/icsa59870.2024.00014

ISO/IEC 27005, (2022) “Information security, cybersecurity and privacy protection — Guidance on managing information security risks”.

Microsoft, (2009) "The STRIDE Threat Model”. Disponível em: <https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)>.

Nakamura, E., Ribeiro, S., (2019) "A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment In a Health IoT System : Results from OCARIoT Project," 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, pp. 1-6, doi: 10.1109/GIOTS.2019.8766364.

NIST. Patrick D. Gallagher, Under Secretary for Standards and Technology and Director. (2012) “Guide for Conducting Risk Assessments: information security”. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

OWASP. Drake, V. (2024) “Threat Modeling”. Disponível em: https://owasp.org/www-community/Threat_Modeling.

Souppaya, M., Montgomery, D., Polk, W., Ranganathan, M., Dodson, D., Barker, W., Johnson, S., Kadam, A., Pratt, C., Thakore, D., et al. (2021). “Securing small-business and home internet of things (iot) devices: Mitigating network-based attacks using manufacturer usage description (mud)”. Technical report, NIST.