risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 03/09/2022
Aceitação/Acceptance: 20/11/2022

Implementação da Arquitetura *Zero Trust*: uma Revisão Sistemática de Literatura

Luiz Guilherme Schiefler de Arruda[1], William Ferreira Giozza[1], Georges Daniel Amvame Nze[1], Rafael Rabelo Nunes[1,2,3]

schiefler@icloud.com; giozza@unb.br; georges@unb.br; rafaelrabelo@unb.br

[1] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP 70910-900 Brasília-DF Brasil

[2] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Administração, CEP 70910-900 Brasília-DF Brasil

[3] Centro Universitário Atenas, Rua Euridamas Avelino de Barros, nº 1400, Prado, CEP 38602-002 Paracatu-MG Brasil

Pages: 261-275

Resumo: O *Zero* Trust (ZT) aparece como uma evolução no conceito de segurança de rede, através da ideia de verificar toda tentativa de acesso à rede, seja pela internet ou intranet. O presente artigo apresenta uma Revisão Sistemática de Literatura, com enfoque voltado à implementação da *Zero Trust Architecture* (ZTA) considerando sete dimensões obtidas da análise dos modelos da Google, Microsoft e NIST. A metodologia PRISMA foi utilizada considerando duas bases de dados: *ACM Digital Library* e *IEEE Xplore* no intervalo entre 2016 e 2022. Quantitativamente, observou-se um aumento no número de artigos no decorrer dos anos, contudo não foi encontrado trabalho com foco na gestão da implementação. Qualitativamente, observou-se uma preocupação maior no tema relacionado ao controle de acesso e identidades e uma ausência de estudos focados na segurança das infraestruturas. Destaca-se, também a falta de trabalhos que apresentem uma priorização na sequência de implementação das dimensões.

Palavras-chave: Segurança Cibernética, *Zero Trust*, Revisão Sistemática de Literatura, PRISMA.

Implementing Zero Trust Architecture: A Systematic Literature Review

Abstract: *Zero Trust (ZT) appears as an evolution in the concept of network security, through the idea of verifying any attempt at network access, whether internet or intranet.* Thus, this paper presents a Systematic Literature Review, focusing on the implementation of Zero Trust Architecture (ZTA), considering seven dimensions obtained from the analysis of the Google, Microsoft, and NIST models. The PRISMA methodology was used considering two databases: ACM Digital Library and IEEE Xplore and the interval between 2016 and 2022. Quantitatively, an increase in the number of articles over the years was observed, however, no

work focusing on implementation management was found. Qualitatively, a greater concern was observed in the theme related to access control and identities and an absence of studies focused on infrastructure security. Also noteworthy is the lack of studies that present a prioritization in the sequence of implementation of the dimensions.

Keywords: *Cybersecurity,* Zero Trust, Systematic Literature Review, PRISMA.

1. Introdução

Algumas mudanças ocorreram na computação empresarial nas últimas duas décadas, principalmente com o surgimento de novas abordagens, como por exemplo a computação em nuvem, a computação de ponta e a Internet das Coisas (IoT, na sigla em inglês) (Vanickis et al., 2018). Além disso, com a proliferação da tecnologia das redes e IoT, observou-se alterações no âmbito dos sistemas de tecnologias da informação (Teerakanok et al., 2021). Com isso, o gerenciamento da segurança das redes tem se tornado um grande desafio, uma vez que os dados são considerados ativos importantes nas instituições (Ahmed et al., 2020). A tradicional segurança de bordas divide a rede entre interna e externa (Chuan et al., 2020; Teerakanok et al., 2021), porém não apresentam capacidade para detectar que dados sejam capturados ou que ataques sejam realizados a partir do interior do próprio perímetro de segurança. Desta maneira, surge um dilema: manter a tradicional segurança de bordas ou mudar para um novo conceito.

Em 2004 a Agência de Sistemas de Informação de Defesa (DISA) e o Departamento de Defesa (DoD) dos EUA, apresentaram um trabalho no Fórum de Jericó, focado na mudança do modelo de segurança de perímetro para um baseado na segurança nas transações (Rose et al., 2020). Em 2010, John Kindervag, enquanto trabalhava como engenheiro da Forrester, aprimorou a ideia de desperimetrização cunhando o que se tornou o *Zero Trust* (ZT) (Rose et al., 2020). O ZT fornece uma coleção de conceitos e ideias projetadas para minimizar a incerteza na aplicação de decisões de acesso precisas e com menos privilégios por solicitação em sistemas e serviços de informação em face de uma rede vista como comprometida (Rose et al., 2020).

Este novo conceito vem ganhando importância tanto que o DoD dos EUA em 2021 publicou uma arquitetura de referência ZT, onde definiu que o ZT deve ser utilizado na priorização e integração de recursos existentes no DoD de maneira a manter a disponibilidade e reduzindo atrasos temporais nos mecanismos de autenticação (Defense Information Systems Agency & National Security Agency, 2021). Também, o *Executive Office of The President* (2022), do governo dos EUA, emitiu um documento determinando que os entes federativos têm até o término do ano fiscal de 2024, para implementar os conceitos e premissas contidas no ZT.

Assim, considerando o fato de ser um conceito relativamente novo e sua relevância observada pelo governo dos EUA, o presente artigo apresenta uma Revisão Sistemática de Literatura (RSL) focada na implementação da *Zero Trust Architecture* (ZTA). Para tal, o trabalho está estruturado da seguinte maneira: na seção 2 será abordado um referencial teórico; na seção 3 será apresentada a metodologia utilizada na realização da revisão sistemática de literatura; na seção 4 serão relatados os resultados obtidos com a revisão da literatura; finalizando com a seção 5, onde são apresentadas as conclusões obtidas com o estudo e propostas de futuros trabalhos.

2. Referencial Teórico

Como uma maneira de nivelar conhecimentos, nesta seção serão apresentados conceitos importantes. Inicialmente, abordar-se-á o conceito ZT, sua arquitetura, as implementações realizadas pelo Google e Microsoft bem como o padrão estabelecido pelo *National Institute of Standards Technology* (NIST).

2.1. Zero Trust

A premissa do ZT é baseada no fato de que nenhum participante da rede é confiável não importando sua localização (Ahmed et al., 2020; Buck et al., 2021; Teerakanok et al., 2021). Com isso, o ZT garante que os acessos sejam verificados em todas as camadas, redes e aplicações dentro de uma corporação, uma vez que a localização deixou de ser considerada o componente principal para verificação da confiança (Campbell, 2020; Kerman et al., 2020).

Dessa forma, o ZT pode ser considerado um paradigma de segurança cibernética focado na proteção de recursos no qual uma organização ou empresa deve assumir que não há uma confiança implícita devendo verificar continuamente cada tentativa de acesso (Ahmed et al., 2020; Rose et al., 2020; Teerakanok et al., 2021).

A ZTA é um plano de segurança cibernética de uma organização que utiliza os conceitos do ZT e abrange relacionamento de componentes, planejamento de fluxo de trabalho e políticas de acesso. Portanto, uma empresa com ZT considera a infraestrutura de rede e as políticas operacionais que estão em vigor como produto de um plano de ZTA (Rose et al., 2020). A ZTA aborda essa tendência concentrando-se na proteção dos recursos, não de perímetros de rede, visto que a localização da rede não é mais considerada o principal componente da postura de segurança necessária (Kerman et al., 2020).

2.1.1. Google BeyondCorp

A implementação do Google para a ZTA partiu de uma nova abordagem para segurança de rede, removendo as necessidades de intranet com privilégios e transferindo suas aplicações para a internet. Para tal, consiste em componentes cooperativos de maneira a garantir que apenas dispositivos e usuários devidamente autenticados sejam autorizados a acessar os aplicativos corporativos necessários (Ward & Beyer, 2014). Como resultado, o objetivo principal do Google foi diminuir a confiança implícita que seus usuários e dispositivos haviam formado por sua presença física ou eletrônica na rede corporativa (Hosney et al., 2022). A Tabela 1 apresenta as cinco dimensões observadas na implementação do Google.

Dimensão	Descrição
Dispositivo	Utilize o conceito de dispositivo gerenciado, onde seja possível obter uma identificação única de cada um, e permita que apenas eles sejam autorizados a acessar seus recursos internos.
Usuário	Gerencie todos seus usuários através de categorização da função exercida, em coordenação com o setor de Recursos Humanos para que mudanças de funções e demissões sejam rapidamente inseridas no Banco de Dados e o acesso seja cancelado ou alterado.

Dimensão	Descrição
Rede	Defina uma rede sem privilégios semelhante à internet com conexão limitada a poucos serviços. Baseado nas informações do dispositivo e usuários, utilize sistemas para atribuir, dinamicamente, o acesso à VLAN correspondente.
Aplicações	Utilize criptografia entre o cliente e a aplicação pois as aplicações estão expostas tanto a rede interna quanto externa.
Controle de Acesso	Defina padrões de acesso aos sistemas e verifique múltiplas fontes de dados para atribuir níveis de confiança ao usuário bem como padrões necessários para acessar sistemas e aplicações.

Tabela 1 – Descrição das dimensões propostas pela Google (Ward & Beyer, 2014).

2.1.2. A ZTA proposta pela Microsoft

Baseado no princípio de sempre verificar as tentativas de acesso, a arquitetura foi refinada no intuito de enfatizar a importância crítica de integração entre automação e a aplicação de políticas, inteligência e proteção contra ameaças através de pilares de segurança. Esses elementos integrados atuam na telemetria em todos os pilares para informar decisões com sinais em tempo real (Microsoft, 2021a). A ZTA proposta na Microsoft é suportada por seis dimensões (Microsoft, 2021b) descritas na Tabela 2:

Dimensão	Descrição
Identidade	Automatize a detecção e a correção de riscos e proteja o acesso a recursos com autenticação forte em todo o patrimônio digital.
Endpoints	Defenda a superfície de ataque maior criada pelo crescente número e diversidade de *endpoints* usando uma abordagem de gerenciamento flexível e integrada.
Rede	Reduza as vulnerabilidades de segurança baseadas em perímetro, incluindo a necessidade de VPNs, e melhore a escalabilidade das soluções de segurança para ambientes onde a nuvem é cada vez mais o centro dos serviços de TI.
Dados	Classifique, rotule e proteja dados em ambientes de nuvem e locais para ajudar a evitar o compartilhamento inadequado e reduzir os riscos internos.
Aplicações	Mantenha o acesso de funcionários altamente seguro a aplicativos móveis e na nuvem, bem como acesso remoto a aplicativos corporativos locais.
Infraestrutura	Proteja a infraestrutura híbrida, incluindo ambientes de TI locais e na nuvem, com gerenciamento mais eficiente e automatizado.

Tabela 2 – Descrição das dimensões propostas pela Microsoft

2.1.3. A ZTA proposta pelo NIST

Segunda Kerman et al. (2020) o NIST foi o primeiro instituto de padronização mundial a escrever os padrões necessárias e uma ZTA.

O Existem três componentes chaves para a ZTA do NIST: (i) o *Policy Engine* (PE) que gera a decisão na autorização, negação ou revogação de um determinado acesso; (ii) o *Policy Administrator* (PA) cuja função principal é estabelecer ou finalizar uma transação entre um sujeito e um recurso; e (iii) o *Policy Enforcement Point* (PEP) onde

são habilitados, monitorados e, eventualmente, encerradas conexões entre sujeitos e recursos corporativos. Algumas implementações podem considerar o PE e PA como um único serviço, realizando nestes casos, as tarefas do PE e PA (Rose et al., 2020).

2.2. Implementação da Arquitetura Zero Trust

Para a implementação da ZTA, precisa-se compreender que a confiança deve ser considerada um atributo bidirecional, estabelecido entre duas entidades, de que a outra entidade é o que afirma ser e que se comportará de maneira esperada durante a duração de interação (Ahmed et al., 2020). Além disso, a confiança pode aumentar as vulnerabilidades a um sistema, principalmente quando esta confiança é gerada de maneira automática.

Baseado nesta confiança e analisando os princípios de Saltzer & Schroeder (1975) observa-se dois que devem ser destacados: Defaults seguros contra falhas, pois ao desenvolver controles de segurança, é importante definir e permitir operações que possam ser positivamente identificadas como estando de acordo com uma política de segurança e rejeitar as demais; e Mediação completa, onde cada acesso aos recursos deve ser verificado e confrontado com as políticas e esquemas de proteção.

Por ser um conceito de segurança mais avançado, sua implementação pode acontecer de diversas maneiras e de acordo com cenários específicos (Buck et al., 2021; Chuan et al., 2020). Conforme observou-se tanto o Google quanto a Microsoft realizaram a implementação do ZT em suas corporações utilizando maneiras diferentes. Aliado a isso, o padrão apresentado pelo NIST apresenta uma outra visão em sua utilização.

A proposta da Google, ilustrada na Figura 1, considera o processo de rastreamento de dispositivos dentro de um banco de dados de dispositivos um ponto basilar em sua segurança. Além disso, o banco de dados de funcionários, gerenciado pelo departamento de recursos humanos, e um serviço de validação de usuários e grupos, permite um sistema de login único. Esses dois serviços atuam de maneira conjunta para autenticar atribuir, dinamicamente, o acesso a VLAN específica. Outro ponto importante da política de acesso proposta está relacionada à atribuição de um nível de confiança do acesso, que ocorre dentro do *Access Proxy*, para permitir, ou não, o acesso a determinado recurso.

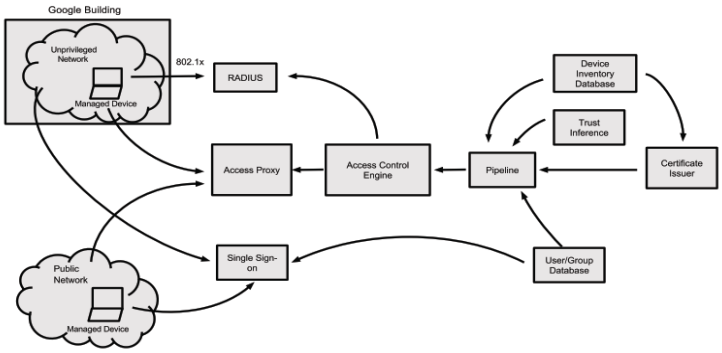

Figura 1 – Componentes do Google BeyondCorp (Ward & Beyer, 2014).

O modelo de ZTA proposto pela Microsoft, representado na Figura 2, considera a Identidade e a conexão através de um *Endpoint* como base de segurança em sua ZTA. As solicitações são recebidas e verificadas pelas Políticas ZT (ZT *Policy*) que, após verificações com elementos fundamentais, impõe acesso com privilégios mínimos. Estas políticas são aprimoradas pela Otimização de Política. Os dados de telemetria e análises, geram avaliações de risco que alimentam o mecanismo de política para oferecer proteção automatizada contra ameaças.

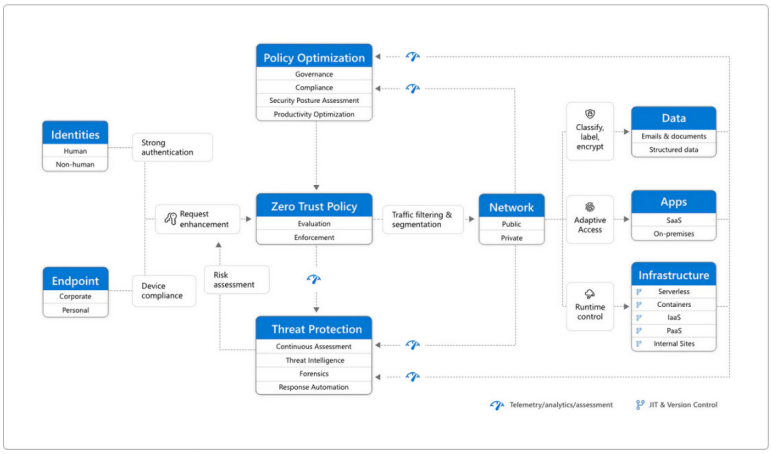

Figura 2 – Diagrama de ZT da Microsoft (Microsoft, 2021a)

A Figura 3 ilustra os diversos componentes lógicos que compões a arquitetura proposta pelo modelo do NIST em uma corporação, sendo observados dois planos básicos: Plano de Dados e Plano de Controle. Enquanto neste ocorrem as transmissões relacionadas as solicitações de acessos, naquele trafegam os controles de acesso (Rose et al., 2020).

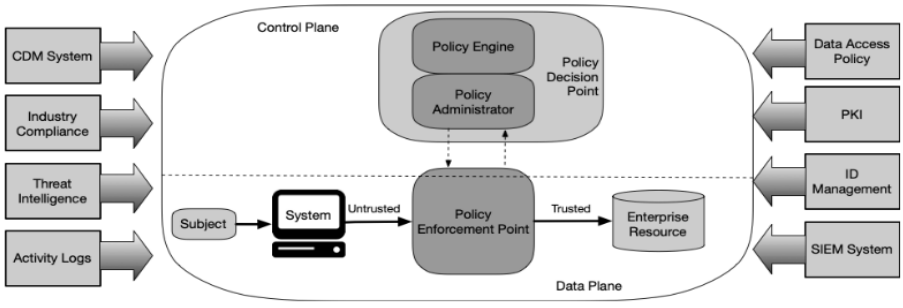

Figura 3 – Modelo de Arquitetura ZT do NIST (Rose et al., 2020)

Desta maneira, analisando as cinco dimensões propostas pela Google e as seis propostas pela Microsoft descritas, observa-se que Controle de Acesso possui relação com Identidade assim como Dispositivo com *Endpoints*. Além disso, ambas utilizam a Rede e Aplicações em suas implementações. Em contrapartida, a proposta do NIST

utiliza três dimensões: uma que trata de autorização ou revogação de uma tentativa de acesso, outra relacionada às conexões entre indivíduos e recursos, e uma terceira onde são habilitadas e monitoradas as conexões. Desta maneira, o presente artigo leva em consideração sete dimensões: Autenticação, Identidade, *Endpoints*, Dados, Rede, Aplicações e Infraestrutura.

3. Metodologia

De forma a identificar as abordagens de implementação do Zero Trust, procedeu-se com uma RSL conduzida pelo método *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA), que em sua última revisão, em 2021, traz um conjunto etapas para realização e um fluxograma que devem ser seguidos na condução de uma revisão sistemática (Galvão & Ricarte, 2019). Dessa forma, o presente trabalho se trata de uma pesquisa exploratória, utilizando uma abordagem qualitativa e quantitativa (Gil, 2002).

Segundo Galvão & Ricarte (2019) uma RSL busca entender e apresentar uma lógica ao grande corpus documental verificando o que funciona ou não em determinado contexto. Uma outra definição pode ser observada em Kitchenham (2004), onde se identifica, avalia e interpreta as pesquisas relevantes disponíveis em uma particular questão de pesquisa de interesse. Além disso, Siddaway et al. (2019) cita como sendo uma das razões para se realizar uma RSL a necessidade de sintetizar um conjunto de evidências sobre um determinado tópico com o propósito de obter conclusões robustas acerca deste assunto.

Na elaboração do trabalho, as bases de dados *IEEE Xplore* e a *ACM Digital* foram utilizadas, pois, segundo Galvão & Ricarte (2019), elas abordam temas relacionados à Tecnologia da Informação. Além disso, sua escolha foi possível visto que o Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes) permite o acesso aos artigos completos publicados. O período considerado na busca foi entre janeiro de 2016 e junho de 2022. Considerando o objetivo do trabalho, ou seja, verificar na literatura as diferentes maneiras de implementação da ZTA, a combinação inicial de palavras foi "Zero Trust" e "*implementation"*. Aliado a isso, utilizou-se as palavras *deployment* e *development* como possíveis sinônimos. Com isso, foram realizadas três pesquisas em casa base de dados: *"zero trust" and implement**, *"zero trust" and develop** e *"zero trust" and deploy**. Utilizou-se o operador "*" ao final das palavras para se ampliar a consulta. O resultado trouxe 268 artigos. Em seguida, foram percorridas as etapas prescritas pelo método PRISMA, conforme mostra a Figura 4.

Dos 268 artigos iniciais retirou-se aqueles duplicados, obtendo, assim, um número de 138 artigos únicos. Na sequência foi realizada a primeira filtragem, que consistiu na verificação dos títulos, resumos e palavras chaves dos artigos com o objetivo de eliminar aqueles que não citaram a expressão Zero Trust em seu título, resumo ou palavras-chave, sendo eliminados 58 artigos. A segunda filtragem buscou retirar artigos indisponíveis e textos de revistas e livros, representando uma redução de 11 documentos. Finalmente o último filtro consistiu na leitura dos resumos na busca de textos não afetos ao tema implementação do ZT. Esta etapa retirou o total de 51 trabalhos, restando. Ao final, 18 artigos foram selecionados.

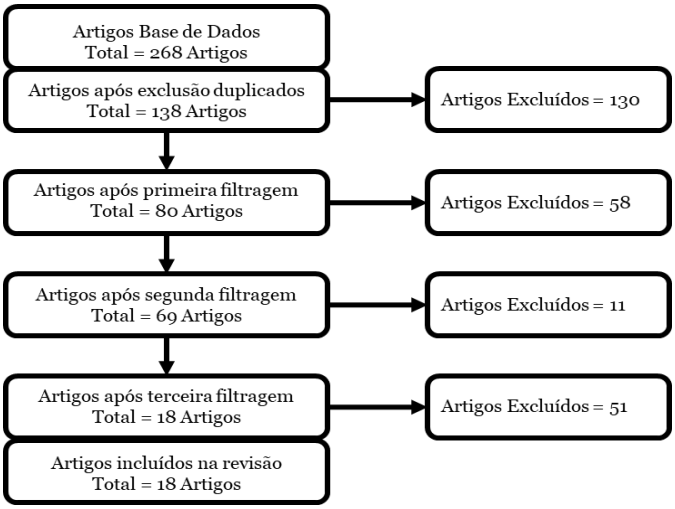

Figura 4 – Fluxograma da revisão.

4. Resultados

Esta seção é dedicada a apresentar os resultados obtidos pela análise da leitura e do estudo dos 18 artigos.

A Tabela 3 apresenta o resultado da classificação dos artigos no que tange às sete dimensões do *Zero Trust* e as respectivas referências para os artigos. Registra-se que um mesmo artigo pode ser classificado em mais de uma dimensão, motivo pelo qual a soma dos percentuais passa de 100%. Pelos resultados obtidos, pode-se observar dedicação maior dos autores em conduzir estudos para as dimensões rede (61%) e autenticação (56%). Em contrapartida, não foi observado trabalho relacionado à dimensão infraestrutura. Em nenhum deles, observou-se trabalhos relacionados no que tange à gestão de uma implementação da ZTA dentro de uma organização. Além disso, apenas dois artigos (Ameer et al., 2022; Chen et al., 2021) abordam cinco ou mais dimensões da implementação, a diferença foi observada visto que o primeiro não aborda a dimensão rede.

Dimensões	Total de Artigos	Autores
Autenticação	10 (56 %)	(Ameer et al., 2022; Bello et al., 2022; Chen et al., 2021; Decusatis et al., 2016; Dimitrakos et al., 2020; D'Silva & Ambawade, 2021; Eidle et al., 2017; Fang & Guan, 2022; Wang et al., 2022; Yao et al., 2020)
Identidade	5 (28 %)	(Ameer et al., 2022; Chen et al., 2021; Hatakeyama et al., 2021; Hosney et al., 2022; Wu et al., 2021)
Endpoints	2 (11 %)	(Ameer et al., 2022; Chen et al., 2021)
Dados	5 (28 %)	(Ameer et al., 2022; Chen et al., 2021; D'Silva & Ambawade, 2021; Fang & Guan, 2022; Wang et al., 2022)

Dimensões	Total de Artigos	Autores
Rede	11 (61 %)	(Chen et al., 2021; da Rocha et al., 2021; Decusatis et al., 2016; D'Silva & Ambawade, 2021; Dzogovic et al., 2022; Fang & Guan, 2022; Hosney et al., 2022; Li et al., 2022; Mujib & Sari, 2020; Wang et al., 2022; Zaheer et al., 2019)
Aplicações	4 (22 %)	(Ameer et al., 2022; Chen et al., 2021; Fang & Guan, 2022; Hosney et al., 2022)
Infraestrutura	0	

Tabela 3 – Visão global dos tópicos.

Frequentemente os artigos abordam a evolução na quantidade de dispositivos de IoT conectados as redes, principalmente aqueles ligados a infraestruturas críticas, devido principalmente, ao aumento da superfície de ataque desse tipo de tecnologia.

Ameer et al., (2022) observam que tanto o *Attribute-Based Access Control* (ABAC) quanto *Role-Based Access Control* (RBAC) não suportam controle contínuo de autorização, bem com o fato de que a tecnologia da Blockchain apresenta características técnicas que podem limitar a aplicabilidade da Blockchain na realização de um controle contínuo de autorização. Assim, os autores avaliam cada um dos sete princípios do ZT baseado no *Policy, Enforcement, Implementation* (PEI) *Framework* para fornecer uma visão estruturada de diferentes requisitos de autorização. Ao final do trabalho, apresentam um conjunto de sete componentes básicos de um modelo de política de autorização ZT, chamado de Framework de Requisitos de Autorização (ZT-ARF, na sigla em inglês).

Chen et al. (2021) apresentam um *framework* de segurança voltado à sistemas médicos inteligentes baseado na ZTA e tecnologia 5G focado em quatro dimensões (ativos, objetos, meio ambiente e comportamento) e uma estrutura que emprega um modelo de controle de acesso dinâmico confiável capaz de decidir, em tempo de execução, os privilégios atinentes a cada acesso. O modelo de controle de acesso é o responsável pela conexão entre o plano de dados e de controle, realizando as avaliações de segurança continuamente e ajusta o privilégio de acesso dinamicamente. Mesmo com os testes realizados no decorrer do estudo, os autores afirmam que ainda existem desafios, principalmente relacionados a uma melhor conscientização das pessoas e possíveis problemas de incompatibilidade com os sistemas 5G existentes na indústria da saúde.

Da Rocha et al. (2021) observaram a inexistência, na literatura, de artigos que utilizem o ZT na prevenção de ataques *Advanced Persistent Threats* (APT). Baseado nisso, simularam uma rede composta de *switches*, roteadores, *firewall* e dispositivos IoT em um cenário onde há um ataque APT em curso. Demonstrou que a microssegmentação com a utilização de NGFW pode ser uma solução na proteção contra esse tipo de ameaça.

D'Silva & Ambawade (2021) descrevem um modelo criado baseado no padrão do NIST. Seu produto utiliza um Servidor de Proxy, cuja função é redirecionar a solicitação de acesso ao servidor de Autenticação e Autorização, porém sua configuração é feita de maneira que o usuário não saiba seu endereço IP real. Foi utilizado a linguagem XACML para desenvolver o sistema de controle de acesso, composto pelo *Policy Administration*

Point (PAP), PDP e PED. Além disso, é apresentado como seu modelo protege cada uma das camadas do modelo *Open System Interconnect* (OSI).

Decusatis et al. (2016) e Eidle et al. (2017) discutiram uma arquitetura única como facilitadora de uma abordagem de ZTA, baseada na geração de um token para identificar uma configuração de rede. Assim, o token de autenticação é ocultado dentro do primeiro pacote de autenticação e solicitações do *Transmission Control Protocol* (TCP). Uma vantagem desta abordagem aparece pois ela simplesmente rejeita as tentativas de acesso negadas, não retornando feedback a um possível usuário mal-intencionado.

Dimitrakos el al. (2020) desenvolvem um novo modelo de autorização contínua através de uma nova tecnologia, mais eficiente e leve, capaz de ser utilizada em redes de IoT, como por exemplo casas inteligentes. Sua eficiência decorre do fato do conceito ZT estar instalado diretamente no dispositivo, reduzindo a quantidade de conexões. A performance do modelo foi avaliada e comparada com a ABAC, apresentando uma melhor eficiência.

Fang & Guan (2022) elaboraram e testaram uma Aplicação iOS para prover uma solução de acesso remoto seguro. Os componentes principais utilizados foram divididos em dois planos com as seguintes tecnologias chaves em cada plano: Plano de Controle (Autenticação baseada em PKI e mecanismo de autorização baseado no RBAC) e Plano de Dados (Mecanismo *Single Package Authorization* (SPA), Transmissão segura de dados baseado em TLCP e acesso a recursos utilizando HTTPS).

Hatakeyama et al. (2021) consideram a utilização de um contexto na realização de verificação de cada acesso em uma ZTA, definindo, assim, a *Zero Trust Federation* (ZTF) de maneira a realizar o controle de acesso através de um servidor de controle de acessos. Este servidor utiliza um protocolo para gerar contextos, contudo, ainda não há uma padronização ou especificação sobre este protocolo.

Hosney et al. (2022) apresentam uma preocupação na limitação de definição de políticas necessárias para mudar de uma proteção através de *firewall* na camada 4, pois, segundo os autorer, o tempo e o esforço necessários na manutenção delas é crucial. Desta maneira, os administradores de rede devem mudar a maneira de pensar na segurança baseada apenas em Fonte, Destino e Aplicação, passando a utilizar o conceito W5H (*Who, What, When, Where, Why and How*). Assim, desenvolvem um estudo de Inteligência Artificial (IA) para definir o motor de política (*Policy Engine*). Seu modelo apresentou uma acurácia de aproximadamente 85%. Além disso, a autenticação, juntamente com o controle de identidades, apresenta-se como uma maneira de garantir acesso a recursos, através da utilização de sistemas de gerenciamento de identidade e credenciais, assim como políticas para acesso a recursos, devendo ser continuamente monitorada.

Em contrapartida Li et al. (2022) nos propõem um framework para verificar pacotes baseados em um SDN e na *blockchain* onde uma estrutura básica de pacote é definida. Assim, torna-se possível uma verificação contínua dos pacotes sem a necessidade de grandes atualizações na infraestrutura.

Mujib & Sari (2020) conduziram simulações para determinar a performance da microssegmentação através da avaliação de três parâmetros: *Round Trip Time* (RTT),

Jitter, perdas de pacotes entre data centers. Estes parâmetros foram comparados em testes realizados na rede sem e com a microssegmentação utilizando o Wireshark. Em que pese haja um acréscimo no tempo do RTT e do *Jitter*, os autores consideraram que a utilização da microssegmentação não afeta a performance da rede.

Wang et al. (2022) descrevem o fato de que mesmo a *blockchain* apresentando altas demandas na verificação de credibilidade, a fragmentação pode aparecer como uma solução de seu problema de escalabilidade.

Em seu artigo Wu et al. (2021) descrevem que existem três formas de verificar a identidade de uma pessoa e baseado nela, apresenta três maneiras na qual a autenticação da identidade pode ser realizada e as vulnerabilidades que cada uma pode apresentar.

Yao et al. (2020) baseando-se no fato que o RBAC não permite que o controle de acesso seja dinâmico, propõem um novo modelo chamado de *Trust-Based Access Control* (TBAC). Este sistema de controle de acesso define e ajusta o status de autorização dinamicamente através de um algoritmo de geração de confiança.

5. Conclusões

Com o propósito de ampliar os conhecimentos acerca da implementação da ZTA, uma revisão sistemática de literatura foi realizada em duas bases de dados voltadas à assuntos afetos a Tecnologia da Informação. Este processo permite descobrir como os tópicos vem sendo abordados pelos pesquisadores, ampliar conhecimentos acerca do assunto, bem como observar possíveis lacunas de estudos.

A partir da leitura dos textos observou-se a preocupação apresentada na forma de autenticação dos usuários, ponto este bastante abordado pelo NIST. Desta maneira, os artigos consideraram estudar sistemas de controle de acesso baseado em Identidades antes de se considerar a localização das redes

Além disso, percebe-se uma preocupação voltada a uma maior compreensão e desenvolvimento de ferramentas e soluções voltadas à autenticação e autorização de acessos a recursos dentro de uma corporação. Aliado a isto, há também, trabalhos relativos a microssegmentação de redes e acesso a estas. Em contrapartida, não foram observados estudos preocupados com o controle das infraestruturas. Este controle, que representa um vetor crítico de ameaças, pode ser aprimorado utilizando ferramentas que apresentem soluções de segurança para proteger a infraestrutura de rede contra-ataques conhecidos e desconhecidos.

Além disto, dentro do espectro de artigos estudados, não foi observado discussões sobre a priorização para implementação dos controles de segurança de uma ZTA, de maneira a garantir um maior nível de confiança no acesso aos recursos.

Desta maneira, torna-se necessário, além de um aprofundamento nos estudos relativos a como garantir uma maior proteção às infraestruturas, um trabalho sobre a priorização dos controles na implementação da ZTA torna-se importante, sendo duas lacunas observadas no decorrer dos estudos, apresentando-se como oportunidades de estudos futuros.

Agradecimentos

Os autores agradecem o suporte da ABIN TED 08/2019. O autor Rafael Rabelo Nunes agradece o suporte do Centro Universitário Atenas e da Universidade de Brasília, por meio do Edital PI/DPG 02/2022.

Referências

Ahmed, I., Nahar, T., Urmi, S. S., & Taher, K. A. (2020). Protection of sensitive data in zero trust model. ACM International Conference Proceeding Series, 0–4. https://doi.org/10.1145/3377049.3377114

Ameer, S., Gupta, M., Bhatt, S., & Sandhu, R. (2022). BlueSky: Towards Convergence of Zero Trust Principles and Score-Based Authorization for IoT Enabled Smart Systems. Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies, 235–244. https://doi.org/10.1145/3532105.3535020

Bello, Y., Refaey, A., Ulema, M., & Kolipali, J. (2022). On Sustained Zero Trust Conceptualization Security for Mobile Core Networks in 5G and Beyond. IEEE Transactions on Network and Service Management, PP(c), 1. https://doi.org/10.1109/TNSM.2022.3157248

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, 110, 102436. https://doi.org/10.1016/j.cose.2021.102436

Campbell, M. (2020). Beyond Zero Trust: Trust Is a Vulnerability. Computer, 53(10), 110–113. https://doi.org/10.1109/MC.2020.3011081

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., & Zhai, Y. (2021). A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture. IEEE Internet of Things Journal, 8(13), 10248–10263. https://doi.org/10.1109/JIOT.2020.3041042

Chuan, T., Lv, Y., Qi, Z., Xie, L., & Guo, W. (2020). An Implementation Method of Zero-trust Architecture. Journal of Physics: Conference Series, 1651(1). https://doi.org/10.1088/1742-6596/1651/1/012010

da Rocha, B. C., de Melo, L. P., & de Sousa, R. T. (2021). Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model. 2021 Workshop on Communication Networks and Power Systems, WCNPS 2021, Wcnps. https://doi.org/10.1109/WCNPS53648.2021.9626270

Decusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M. (2016). Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication. Proceedings - 2016 IEEE International Conference on Smart Cloud, SmartCloud 2016, 5–10. https://doi.org/10.1109/SmartCloud.2016.22

Defense Information Systems Agency, & National Security Agency. (2021). Department of Defense (DoD) Zero Trust Reference Architecture. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

Dimitrakos, T., Dilshener, T., Kravtsov, A., la Marra, A., Martinelli, F., Rizos, A., Rosett, A., & Saracino, A. (2020). Trust aware continuous authorization for zero trust in consumer internet of things. Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020, 1801–1812. https://doi.org/10.1109/TrustCom50675.2020.00247

D'Silva, D., & Ambawade, D. D. (2021). Building A Zero Trust Architecture Using Kubernetes. 2021 6th International Conference for Convergence in Technology, I2CT 2021, 1–8. https://doi.org/10.1109/I2CT51068.2021.9418203

Dzogovic, B., Santos, B., Hassan, I., Feng, B., Do, V. T., Jacot, N., & van Do, T. (2022). Zero-Trust Cybersecurity Approach for Dynamic 5G Network Slicing with Network Service Mesh and Segment-Routing over IPv6. 105–114. https://doi.org/10.1109/das54948.2022.9786074

Eidle, D., Ni, S. Y., Decusatis, C., & Sager, A. (2017). Autonomic security for zero trust networks. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017, 2018-Janua(Area 4), 288–293. https://doi.org/10.1109/UEMCON.2017.8249053

Executive Office of The President. (2022). Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. Executive Office of the President Office of Management and Budget, 26633(January), 1–29. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Fang, W., & Guan, X. (2022). Research on iOS Remote Security Access Technology Based on Zero Trust. IEEE 6th Information Technology and Mechatronics Engineering Conference, ITOEC 2022, 238–241. https://doi.org/10.1109/ITOEC53115.2022.9734455

Galvão, M. C. B., & Ricarte, I. L. M. (2019). REVISÃO SISTEMÁTICA DA LITERATURA: CONCEITUAÇÃO, PRODUÇÃO E PUBLICAÇÃO. Logeion: Filosofia Da Informação, 6(1), 57–73. https://doi.org/10.21728/logeion.2019v6n1.p57-73

Gil, A. C. (2002). Como Elaborar Projetos de Pesquisa (4th ed.). Editora Atlas.

Hatakeyama, K., Kotani, D., & Okabe, Y. (2021). Zero Trust Federation: Sharing Context under User Control towards Zero Trust in Identity Federation. 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events, PerCom Workshops 2021, 514–519. https://doi.org/10.1109/PerComWorkshops51409.2021.9431116

Hosney, E. S., Halim, I. T. A., & Yousef, A. H. (2022). An Artificial Intelligence Approach for Deploying Zero Trust Architecture (ZTA). 5th International Conference on Computing and Informatics, ICCI 2022, 343–350. https://doi.org/10.1109/ICCI54321.2022.9756117

Kerman, A., Borchert, O., Rose, S., Division, E., & Tan, A. (2020). Implementing a Zero Trust Architecture. Nist, October.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. Jt. Tech. Report, Keele Univ. TR/SE-0401 NICTA TR- 0400011T.1, 33, 33. https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

Li, Z., Ding, Y., Gao, H., Qu, B., Wang, Y., & Li, J. (2022). A Highly Compatible Verification Framework with Minimal Upgrades to Secure An Existing Edge Network. ACM Transactions on Internet Technology. https://doi.org/10.1145/3511901

Microsoft. (2021a). Evolving Zero Trust: How real-world deployments and attacks are shaping the future of Zero Trust strategies. https://www.microsoft.com/pt-br/security/business/zero-trust

Microsoft. (2021b). The Comprehensive Playbook for Implementing Zero Trust Security. https://clouddamcdnprodep.azureedge.net/gdc/gdctT4SO0/original

Mujib, M., & Sari, R. F. (2020). Performance Evaluation of Data Center Network with Network Micro-segmentation. ICITEE 2020 - Proceedings of the 12th International Conference on Information Technology and Electrical Engineering, 27–32. https://doi.org/10.1109/ICITEE49829.2020.9271749

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. In Encyclopedia of Cryptography, Security and Privacy. Springer Berlin Heidelberg. https://doi.org/10.6028/NIST.SP.800-207

Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. Proceedings of the IEEE, 63(9), 1278–1308. https://doi.org/10.1109/PROC.1975.9939

Siddaway, A. P., Wood, A. M., & Hedges, L. v. (2019). How to Do a Systematic Review: A Best Practice Guide for Conducting and Reporting Narrative Reviews, Meta-Analyses, and Meta-Syntheses. Annual Review of Psychology, 70, 747–770. https://doi.org/10.1146/annurev-psych-010418-102803

Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust Architecture: Reviews and Challenges. Security and Communication Networks, 2021. https://doi.org/10.1155/2021/9947347

Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B. (2018). Access Control Policy Enforcement for Zero-Trust-Networking. 29th Irish Signals and Systems Conference, ISSC 2018. https://doi.org/10.1109/ISSC.2018.8585365

Wang, J., Chen, J., Xiong, N., Alfarraj, O., Tolba, A., & Ren, Y. (2022). S-BDS: An Effective Blockchain-based Data Storage Scheme in Zero-Trust IoT. ACM Transactions on Internet Technology. https://doi.org/10.1145/3511902

Ward, R., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. ;;Login:, 39(6), 6–11. https://www.usenix.org/publications/login/dec14/ward

Wu, Y. G., Yan, W. H., & Wang, J. Z. (2021). Real identity-based access control technology under zero trust architecture. Proceedings - 2021 International Conference on Wireless Communications and Smart Grid, ICWCSG 2021, 18–22. https://doi.org/10.1109/ICWCSG53609.2021.00011

Yao, Q., Wang, Q., Zhang, X., & Fei, J. (2020). Dynamic Access Control and Authorization System based on Zero-trust architecture. ACM International Conference Proceeding Series, 123–127. https://doi.org/10.1145/3437802.3437824

Zaheer, Z., Chang, H., Mukherjee, S., & Merwe, J. van der. (2019). EZTrust: Network-Independent Zero-Trust Perimeterization for Microservices. SOSR 2019 - Proceedings of the 2019 ACM Symposium on SDN Research, 49–61. https://doi.org/10.1145/3314148.3314349