RBTI – Revista Brasileira em Tecnologia da Informação
Volume 06, número 01 – 2024
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

Arquitetura *Zero Trust*: boas práticas de gestão de riscos de segurança da informação.

Eduardo Nascimento
FATEC Americana
João Emmanuel S'Alkmin Neves
FATEC Americana, joao.neves11@fatec.sp.gov.br

RESUMO

O presente artigo discorre sobre o modelo ZTA, cuja abordagem consiste na confiança zero, no que tange à gestão de riscos de segurança da informação. A revisão bibliográfica permite a disseminação do conceito, e a compreensão detalhada dos princípios e da composição da arquitetura Zero Trust. Acompanhada da análise de boas práticas encontradas atualmente, evidencia-se as vantagens e os benefícios de sua implantação, e ainda se apresentam as dificuldades, desde a aceitação de um novo paradigma por parte de gestores, quanto a mobilização para a introdução de uma nova cultura e estratégia, sem negligenciar o investimento necessário para colocar este modelo em prática. Ao final do trabalho as considerações sobre os desafios futuros e algumas sugestões, afinal o modelo não encerra em si mesmo, é adaptado e adaptável às necessidades e às particularidades de cada corporação, quanto ao acesso aos dados, exigindo a melhoria contínua de sua estrutura e processos.

Palavras-chave: Arquitetura; Confiança zero; Gestão de riscos; Organizações; Segurança de rede.

Data de Submissão: 14/11/2023

Data Aceito Publicação: 15/05/2024

Zero Trust Architecture: best practices for managing information security risks.

ABSTRACT

This article discusses the ZTA model, whose approach consists of zero trust, regarding information security risk management. The bibliographic review allows the dissemination of the concept, and a detailed understanding of the principles and composition of the Zero Trust Architecture. Accompanied by the analysis of good practices currently found, the advantages and benefits of its implementation are highlighted, and difficulties are still presented, since the acceptance of a new paradigm by managers, to the mobilization for the introduction of a new culture and strategy, without neglecting the investment necessary to put this model into practice. At the end of the work, considerations about future challenges and some suggestions, after all the model does not close in itself, it is adapted and adaptable to the needs and particularities of each corporation, in terms of access to data, requiring continuous improvement of its structure and processes.

Keywords: Architecture; Enterprises; Network security; Risks Management; Zero trust.

1 INTRODUÇÃO

No cenário atual, com a rápida evolução digital, as organizações enfrentam o desafio de protegerem seus dados e sistemas sensíveis contra ameaças cibernéticas, que se tornam proporcionalmente cada vez mais frequentes e sofisticadas.

Segundo dados da Fortinet (2023), no ano de 2022 houve mais de 360 bilhões de tentativas de ciberataques somente na América Latina e Caribe, sendo o México o país com maior número, 187 bilhões de tentativas, seguido do Brasil com 103 bilhões.

Os modelos tradicionais de segurança da informação, nos quais predomina a implantação de sistemas de defesa em perímetro, revelam-se inadequados diante do avanço dos métodos de ataques.

Por essa razão, um número cada vez maior de organizações começa a adotar novas formas de abordagem na segurança de seus ativos, com medidas efetivas e abrangentes, que buscam desenvolver o Sistema de Gestão de Segurança da Informação (SGSI) e, consequentemente, melhorar os processos de mitigação de riscos e ameaças, oriundas tanto do ambiente externo quanto interno, bem como da infraestrutura de tecnologia da informação. Assim, desponta como uma solução adequada e estratégica, a *Zero Trust Architecture* (ZTA).

Este artigo discorre sobre a implantação crítica da Arquitetura *Zero Trust* como um novo modelo e paradigma, uma mudança de mentalidade e de gestão de riscos de segurança da informação, ao trazer os princípios e as estratégias fundamentais concernentes à estrutura ZTA. Utiliza-se da revisão bibliográfica sobre o tema, e tem como objetivo geral, contribuir com ideias para as organizações protegerem seus dados e sistemas de maneira eficaz. Como objetivo específico, apresenta três casos reais de empresas renomadas, trazendo o que há de mais novo na área, com a finalidade de confrontar teoria e prática, comprovar os fatos, justificando pesquisas substanciais e fomento a um assunto tão emergente.

2 ZERO TRUST: CONCEITOS, PRINCÍPIOS E COMPOSIÇÃO

Em uma rede na qual a estrutura delimita sua segurança em perímetro, com a utilização de um conjunto de ativos de segurança como *firewall*, servidores de autenticação como RADIUS, pela aplicação do protocolo 802.1X etc., presume-se que todo acesso autorizado por estes filtros sejam de origem confiável e podem, a partir de então, obterem acesso a toda rede de acordo com o nível de permissão definido pelo servidor. Porém, autorizado o acesso, ignora-se qualquer ação que possa gerar vulnerabilidades e trazer riscos ou ameaças como consequência, seja intencionalmente ou não.

Nessa medida, pensando na possibilidade de invasão da rede e na obtenção de acesso aos ativos de tecnologia da informação, quando um atacante consegue permear as defesas e conseguir acesso, ele tem a possibilidade de movimento lateral dentro da rede – o que não é detectado pelas defesas perimetrais já que o acesso foi autorizado – e, assim, tentar elevar seu nível de permissão até que consiga acesso como administrador da rede.

Isso se tornou um grande problema para as organizações, já que os processos gerenciais para a manutenção de uma rede segura passaram a requerer maior cuidado e esforço contínuo de planejamento e gestão. Além disso, devido à disseminação da

computação em nuvem, dos dispositivos móveis e do trabalho remoto e, especialmente, na atual situação em que os dados e informações se tornaram ativos mais valiosos e o mundo cada vez mais global e digital, o modelo de defesa por perímetro mostrou-se inadequado, para não dizer obsoleto.

Partindo destas adversidades criou-se o conceito de desperimetralizar e, em seguida, o termo "confiança zero" na segurança cibernética passou a ser adotado como um novo paradigma de arquitetura e gerenciamento dos ativos de tecnologia da informação.

Na norma NIST 800-207 da *National Institute of Standards and Technology*, Rose et al (2020), descreve a arquitetura de confiança zero (ZTA) como um plano de segurança cibernética empresarial que utiliza conceitos de confiança zero e abrange relacionamentos de componentes, planejamento de fluxo de trabalho e políticas de acesso. Uma empresa de confiança zero é a infraestrutura de rede (física e virtual) e as políticas operacionais que estão em vigor para a empresa como produto de um plano de arquitetura de confiança zero (ROSE *et al*, 2020).

Entende-se como confiança zero, ou *Zero Trust* (ZT), o processo que desenvolve um conjunto de ideias e princípios com o intuito de reduzir a incerteza na aplicação de decisões que restringem e limitam o acesso a sistemas e serviços de informação dentro de um ambiente de rede que possa estar comprometido (ROSE *et al*, 2020).

Esse processo parte, basicamente, da solicitação de acesso a um recurso (sistema, dados ou aplicação) onde a origem é uma zona não confiável, que por sua vez passa por um ponto de decisão de políticas a serem atribuídas e possa ter acesso a um recurso dentro de uma zona implicitamente confiável. A NIST apresenta um modelo abstrato que ajuda a compreender como se dá o acesso a uma zona *Zero Trust*.

A partir deste conceito, baseia-se a confiança zero no princípio de "nunca confiar, sempre verificar", ou seja, a confiança nunca deve ser automaticamente assumida ou presumida por qualquer usuário, dispositivo ou sistema, independentemente da sua localização na rede e do seu nível de permissão de acesso; ao contrário, deve ser enfatizada a verificação contínua da identidade e da conduta de segurança antes da concessão de acesso aos recursos.

Rose *et al* (2020) esclarecem que, uma arquitetura de confiança zero é projetada e implantada com adesão aos seguintes princípios básicos, a saber:

a. **Todas as fontes de dados e serviços computacionais são considerados recursos.** Uma rede pode ser composta por múltiplas classes de dispositivos e ter dispositivos pequenos que enviam dados para agregadores/armazenamento, software como serviço (SaaS), sistemas que enviam instruções para atuadores e outras funções.
b. **Toda comunicação é protegida independentemente da localização da rede**. A confiança não deve ser concedida automaticamente com base no fato de o dispositivo estar na infraestrutura de rede corporativa. Toda comunicação deve ser feita da maneira mais segura disponível, protegendo a confidencialidade e a integridade e fornecendo autenticação da fonte.
c. **O acesso a recursos empresariais individuais é concedido por sessão.** A confiança no solicitante é avaliada antes que o acesso seja concedido. O acesso também deve ser concedido com o mínimo de privilégios necessários para concluir a tarefa. A

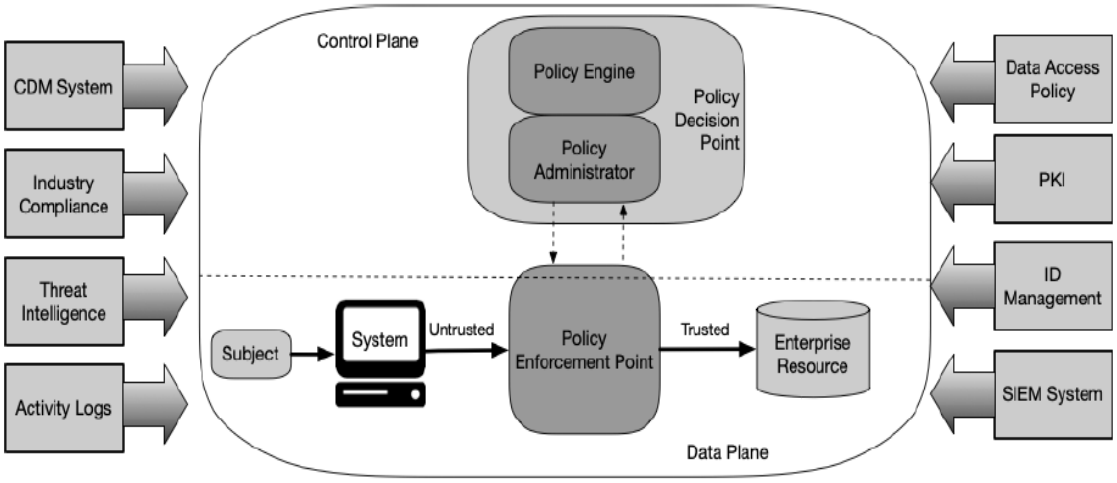
autenticação e a autorização para um recurso não serão concedidas automaticamente a um recurso diferente.

d. **O acesso aos recursos é determinado por políticas dinâmicas, incluindo o estado observável da identidade do cliente, da aplicação/serviço e do ativo solicitante, e englobar outros atributos comportamentais e ambientais**. A organização define como será feita a proteção de seus recursos e membros e delimita o acesso a eles, conforme suas necessidades de acesso. Para confiança zero, a identidade do cliente pode incluir a conta do usuário (ou identidade de serviço) e quaisquer atributos associados concedidos pela empresa. A solicitação do estado do ativo pode incluir características do dispositivo, como versões de software instaladas, localização da rede, hora/data da solicitação, comportamento observado anteriormente e credenciais instaladas. Os atributos comportamentais incluem análises automatizadas de assuntos, análises de dispositivos e desvios medidos dos padrões de uso. Essas regras e atributos são baseados nas necessidades do processo de negócios e no nível aceitável de risco.
e. **A empresa monitora e mede a integridade e a postura de segurança de todos os ativos próprios e associados**. Nenhum ativo é inerentemente confiável. A empresa avalia a postura de segurança do ativo ao avaliar uma solicitação de recurso. Uma empresa que implemente uma ZTA deve estabelecer um diagnóstico e mitigação contínuos (CDM) ou sistema semelhante para monitorar o estado de dispositivos e aplicativos e aplicar *patches*/correções conforme necessário. Os ativos descobertos como subvertidos, com vulnerabilidades conhecidas e/ou não gerenciados pela empresa podem ser tratados de maneira diferente. Isto também se aplica a dispositivos associados, por exemplo, dispositivos de propriedade pessoal, que podem ter permissão para acessar alguns recursos, mas não outros, e requerem um sistema robusto de monitoramento.
f. **Toda autenticação e autorização de recursos são dinâmicas e rigorosamente aplicadas antes que o acesso seja permitido**. Este é um ciclo constante de obtenção de acesso, verificação e avaliação de ameaças, adaptação e reavaliação contínua da confiança na comunicação. Espera-se que uma empresa que implemente uma ZTA possua sistemas de gerenciamento de identidade, credenciais e acesso, e de gerenciamento de ativos em funcionamento, incluindo o uso de autenticação multifator, e o monitoramento contínuo com possível reautenticação e reautorização durante as transações do usuário, a fim de se alcançar um equilíbrio entre segurança, disponibilidade, usabilidade e eficiência de custos.
g. **A empresa coleta o máximo de informações possível sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as utiliza para melhorar sua postura de segurança**. A empresa deve coletar dados sobre a postura de segurança de ativos, tráfego de rede e solicitações de acesso, processar esses dados e usar o conhecimento obtido para melhorar a criação e aplicação das políticas (ROSE *et al*, 2020).

Existem ainda vários componentes lógicos que constituem uma implantação ZTA em uma empresa. Esses componentes podem ser operados como um serviço local ou por meio de um serviço baseado em nuvem (ROSE *et al*, 2020).

A seguir, o esquema de arquitetura ZTA e as considerações quanto aos componentes lógicos que contemplam a sua estrutura.

Figura 1 - Modelo *Zero Trust* do NIST 800-207 e seus componentes lógicos.



Fonte: ROSE *et al*, 2020.

Os componentes apresentados correspondem a uma estrutura principal de controle (*Control Pane*) contendo o Mecanismo de Política ou *Policy Engine* (PE), responsável pela decisão final de concessão de acesso a um recurso para determinado sujeito, utilizando políticas organizacionais, entradas e fontes externas, e o Administrador de Políticas ou *Policy Administrator* (PA), destinado a estabelecer e/ou interromper a comunicação dos recursos, gerando uma sessão específica de autenticação/autorização de um cliente para com o recurso organizacional. O PA está diretamente ligado ao PE e depende deste para conceder ou negar acesso solicitado pelo Ponto de Aplicação de Políticas (ROSE *et al*, 2020).

O Ponto de Aplicação de Políticas ou *Policy Enforcement Point* (PEP) é responsável por habilitar, monitorar e eventualmente finalizar a conexão entre o sujeito e o recurso, além de repassar requisições ao Administrador de Políticas (PA) e deste receber atualizações de políticas. É o componente que está entre o Sistema (não confiável) e os Recursos Organizacionais (confiáveis) (idem, 2020).

Juntamente com os componentes principais da ZTA, há uma série de fontes de dados que provêm políticas e regras de entrada que dão suporte às decisões de concessão de acesso. São compostas pelo Sistema Contínuo de Diagnósticos e Mitigação (CDM), Sistema de Conformidade de Indústria, *Feeds* de Inteligência Sobre Ameaças, *Logs* de Atividade da Rede e Sistema, Políticas de Acesso a Dados, Infraestrutura de Chave Pública Corporativa (PKI), Sistema de Gestão de Identidade (ID) e Sistema de gerenciamento de informações e eventos de segurança (SIEM) (ibidem, 2020).

Para Rose *et al* (2020), uma empresa pode implementar uma arquitetura ZTA de diversas maneiras, de acordo com os seus fluxos de trabalho, variando conforme os componentes utilizados e a principal fonte de políticas e regras para a organização, podendo variar também conforme a abordagem *Zero Trust* que se pretenda implementar, ou ainda utilizando uma solução que contemple uma ou duas abordagens, ou de forma

completa, com as três abordagens existentes, que incluem a governança aprimorada de identidade, a microsegmentação lógica e a segmentação baseada em rede.

3 PROCEDIMENTOS METODOLÓGICOS

Como metodologia para a produção deste artigo adotou-se a pesquisa bibliográfica, exploratória e de abordagem qualitativa.

Partindo-se da revisão da literatura sobre o tema, tão em voga atualmente, quanto ainda carente de publicações, foram consultados manuais técnicos e artigos científicos, assistidos vídeos e palestras que abordam o assunto, analisados exemplos de empresas que utilizam a arquitetura ZTA e oferecem plataformas para a sua implantação.

Segundo Marconi e Lakatos (2003), a pesquisa bibliográfica não é mera repetição do que já foi escrito sobre determinado assunto, propiciando examiná-lo sob um novo enfoque, chegando-se a considerações inovadoras.

Não se optou por um estudo de caso específico, mas por encontrar boas práticas no mercado, revelar a vantagem competitiva e os benefícios que a arquitetura ZTA promovem, já que o conceito é relativamente novo e o assunto mostra-se relevante dentro das corporações e no mundo cada vez mais conectado e ávido por informações.

A pesquisa exploratória tem como propósito desenvolver, esclarecer e até transformar conceitos e ideias, e apresenta menor rigidez no planejamento; é orientada no sentido de favorecer uma visão geral, aproximativa, acerca de determinados fatos (GIL, 1999). Malhotra (2001) complementa que, este tipo tem como características um processo de pesquisa flexível e não-estruturado, uma amostra pequena e não-representativa, a observação informal, uma análise de dados qualitativa, constatações experimentais e resultados, geralmente, seguidos por outras pesquisas futuras.

A abordagem qualitativa foi escolhida para explicar a origem, a premissa, as relações e a mudança que este paradigma traz para a questão do gerenciamento de riscos, investigando diretamente a situação, obtendo dados descritivos, enfatizando mais o processo que o produto; o interesse do pesquisador ao estudar a Arquitetura *Zero Trust* é verificar como se manifesta nas atividades, nos procedimentos e nas interações cotidianas, induzindo as consequências (observam-se os dados e se supõe).

4 RESULTADOS E DISCUSSÃO

A arquitetura *Zero Trust* possui uma abordagem que vai além da concepção física, mobiliza mudanças na estrutura e no desenvolvimento dos processos, alcançando um valor estratégico para as organizações. Consequentemente, seu modelo traz benefícios quando aplicado de maneira integral e abarcando tudo aquilo que compõe ativos da empresa.

Torna-se, assim, um componente crucial para a mitigação de vulnerabilidades, riscos e ameaças, pois estrutura todo o contexto dentro de uma empresa no processo de proteção, monitoramento e análise de identidades, acessos e dados. Além disso, atua no processo de melhoria contínua, corrigindo pontos fracos e aperfeiçoando pontos fortes, tendo como base o estabelecendo de métricas de níveis de criticidade dos ativos.

Dando subsídios à fundamentação teórica, nesse momento apresenta-se casos reais de boas práticas de implementação da arquitetura ZT por organizações. Far-se-á a análise das empresas **AWS**, **Google** e **Microsoft**.

A *Amazon Web Services* (AWS) possui soluções de serviços e recursos que podem ser usados para implementar uma arquitetura *Zero Trust*. Gooden (2023) destaca esses serviços:

a. **AWS *Identity and Access Management* (IAM):** fornece controles de autenticação e autorização para usuários, grupos e recursos, incluindo *single-sign-on* (SSO), autenticação multifator (MFA), entre outros;
b. **AWS *Network Access Control Lists* (ACLs):** permite que se controle o tráfego de rede entre recursos, é uma solução aplicada à microsegmentação, auxiliando a empresa a isolar e proteger dados e sistemas críticos de acessos não autorizados;
c. **AWS *CloudTrail*:** registra todas as solicitações de API, o que pode ser usado no controle do armazenamento *cloud*, na detecção e remediação de atividades suspeitas;
d. **AWS *Security Hub*:** responsável por centralizar e automatizar buscas, fornecendo uma visão geral de sua postura de segurança e ajuda a identificar vulnerabilidades.

Ele também indica uma abordagem em fases para a implementação de uma arquitetura *Zero Trust*. As principais etapas são: identificação de todos os ativos que precisam ser protegidos, incluindo dados, sistemas e aplicativos; implementação de controles de autenticação e autorização rigorosos para garantir que apenas usuários e dispositivos autorizados possam acessar recursos; segmentação de rede em micro perímetros, limitando o acesso a recursos confidenciais; implementação de controles de acesso granulares para cada recurso; e monitoramento e análise do tráfego da rede para detectar atividades suspeitas.

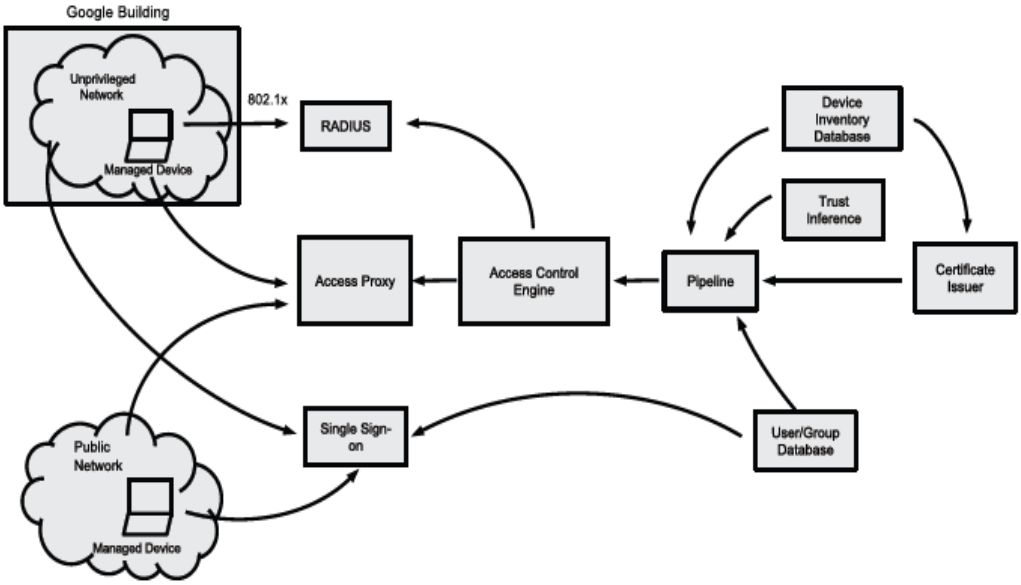
Gooden (2023) relaciona os próximos passos após a implementação e concepção de um modelo *Zero Trust*: implementar o plano adotado, implantar efetivamente a ZTA, realizar avaliações regulares de segurança e otimizar continuamente o ambiente de nuvem e os controles de segurança.

Além da abordagem e dos serviços disponíveis, a AWS orienta e fornece recursos para auxiliar as organizações a implementarem uma arquitetura ZT, bem como fornece serviços de consultoria e implantação que podem ajudar as organizações a otimizarem o processo.

A segunda empresa, a Google, foi uma das empresas pioneiras em adotar *Zero Trust* em sua infraestrutura, com o desenvolvimento da *BeyondCorp Enterprise*. Essa ferramenta destina-se à capacitação das empresas para adoção da abordagem *Zero Trust*, reunindo informações sobre um usuário, levando em conta o contexto de qual dispositivo e local este usuário está localizado e, assim, possibilitando que uma empresa tome decisões de acesso e aplique as políticas de segurança adequadas.

Em todo processo de verificação são analisadas ameaças, fluxos de conexões e acesso, e realizadas aplicações de políticas baseadas em identidade e contexto, como se observa na figura abaixo.

Figura 2 – Componentes e fluxo de acesso da *BeyondCorp Enterprise*



Fonte: WARD, R; BEYER, B., 2014.

A arquitetura *Zero Trust* da Google baseia-se em três pilares principais: autenticação forte, na qual usuários e dispositivos devem ser autenticados de forma segura antes de serem autorizados a acessar recursos; controle de acesso baseado em risco, ou seja, o acesso é concedido de acordo com o usuário, dispositivo ou requisição; e na visibilidade e análise, que requer que as empresas tenham uma visão de todos os seus ativos e do tráfego para poderem detectar e responder às ameaças.

Entre as tecnologias utilizadas pela *BeyondCorp Enterprises*, alinhadas aos pilares descritos acima, estão a gestão de identidade e acesso (IAM), usada para gerenciar identidades e credenciais de usuários; a gestão de dispositivos, destinada à verificação da segurança e a conformidade dos dispositivos; a microsegmentação, usada para dividir a rede em pequenas áreas, o que dificulta para os atacantes se moverem lateralmente; a inteligência de ameaças, aplicada na identificação e resposta a ameaças em tempo real; e a autenticação forte, com a autenticação multifator (MFA), que consiste na utilização de duas ou mais formas de autenticação, como uma senha, um código de verificação ou impressão digital, a autenticação baseada em identidade, baseada em informações sobre o usuário, como seu cargo ou departamento, para determinar seu nível de acesso, e a autenticação baseada em dispositivo, para determinar se ele é seguro.

Há ainda o controle de acesso baseado em risco, que engloba uma variedade de fatores que determinam o nível de risco de uma requisição de acesso, como a identidade do usuário (usuários com acesso a informações confidenciais ou sistemas críticos são considerados de alto risco), o dispositivo do usuário (dispositivos não seguros ou não

conformes são considerados de alto risco), e tempo e local da solicitação (solicitações de acesso de fora da organização ou em horários incomuns são consideradas de alto risco).

Quanto à visibilidade e análise, utiliza uma série de ferramentas e técnicas que permitem visualizar todos os seus ativos e tráfego, incluindo o monitoramento de rede, registrando todo o tráfego, a inteligência de ameaças, identificando ameaças conhecidas e emergentes, e análise de comportamento anormal, que identifica atividades suspeitas.

A implementação da arquitetura *Zero Trust* pela *BeyondCorp Enterprises* segue um processo gradual que se divide em três etapas fundamentais. A primeira, a planificação, consiste em definir os objetivos de segurança e identificar os recursos e tecnologias necessários para implementá-los. Em seguida, a implantação, fase na qual a organização deve implantar a infraestrutura e as políticas de segurança necessárias para a arquitetura. E, por último, a operação e gerenciamento, para monitorar e gerenciar a arquitetura *Zero Trust* de forma a garantir que ela funcione como o esperado.

Ao implementar as boas práticas conforme apresentado pela *BeyondCorp*, a empresa apresenta alguns benefícios para as organizações como a redução dos riscos de ataques, a melhoria da segurança em trabalho remoto e redução de custos de segurança, eliminando a necessidade de VPNs e de outras tecnologias tradicionais.

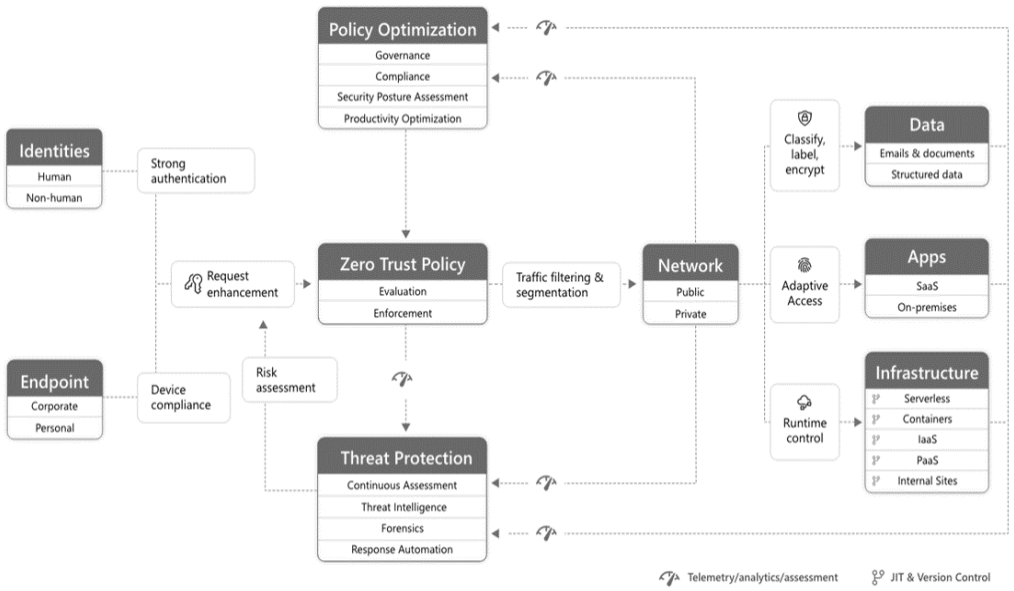
Em 2020, com a pandemia atingindo o mundo todo e o isolamento social, as organizações se viram obrigadas a adotar a estratégia *Zero Trust*, já que pela quantidade de funcionários atuando remotamente, redes privadas virtuais (VPNs) foram violadas ou sobrecarregadadas. A transformação digital tornou-se fator crucial para a sustentabilidade dos negócios (MICROSOFT, 2021).

Com a adoção do modelo *Zero Trust*, a Microsoft ajudou organizações do mundo todo a desenvolverem suas implantações de ZT para comportar as transições para o trabalho remoto e, após o controle da pandemia, com o sistema de trabalho híbrido, em paralelo a uma crescente intensidade e sofisticação dos ataques cibernéticos.

Dentro deste contexto, a Microsoft desenvolveu uma arquitetura baseada em princípios que guiam o modelo *Zero Trust*, que compreendem:

a. **Verificar explicitamente:** sempre tomar decisões de segurança usando todos os dados disponíveis, como localização, identidade, integridade do dispositivo, recurso, classificação de dados e anomalias;
b. **Usar acesso com menos privilégios:** limitar o acesso com o modelo *just-in-time* e *just-enough-access,* apenas o suficiente (JIT/JEA), e políticas adaptativas baseadas em risco.
c. **Assumir violação:** reduzir ao máximo o raio de ação de ataques utilizando microssegmentação, criptografia final de ponta a ponta, monitoramento contínuo e detecção e resposta automatizada a ameaças.

Figura 3 – Componentes da arquitetura *Zero Trust* da Microsoft



Fonte: MICROSOFT, 2021.

Partindo de um modelo de maturidade, a empresa define três etapas para que uma organização questione e analise ao aplicar a arquitetura *Zero Trust*, começando pelo primeiro estágio, no qual deve-se questionar se há redução de riscos em senhas com a adoção de métodos fortes como a autenticação multifator (MFA) e a adoção de *single-sign-on* (SSO) para o acesso a aplicações na nuvem (MICROSOFT, 2021). Em seguida, o processo mais significativo e que envolve questionamentos mais avançados, como se há a utilização de análises em tempo real para avaliar o comportamento dos usuários e a integridade dos dispositivos, se é possível fazer relação entre os sinais de segurança dentre os seus pilares *Zero Trust* para detectar ameaças e agir rapidamente e se é possível encontrar e corrigir de forma proativa as vulnerabilidades como configurações incorretas e *patches* ausentes para reduzir os vetores de ameaça (idem, 2021).

Por fim, com o avanço da maturidade, objetivando metas de otimização do processo, questionar se é possível aplicar dinamicamente políticas após a concessão do acesso para a proteção contra violações, se o ambiente está protegido usando a detecção automatizada de ameaças e respostas para reagir mais rapidamente às ameaças avançadas, e se há análise da produtividade e sinais de segurança para que auxiliem a direcionar o usuário na melhora de sua experiência e compreensão (ibidem, 2021).

É importante salientar que a arquitetura *Zero Trust* é um modelo dinâmico e, como já dito anteriormente, de melhoria contínua. Por esta razão, em sua implementação, a Microsoft espera que as organização obtenham como resultados: uma mudança de conceito de proteção dos pilares individuais com as políticas e controles corretos para a unificação de todos os setores, estabelecendo uma integração mais profunda, uma aplicação consistente e uma proteção holística; a inteligência contra ameaças, a resposta automatizada e a priorização dos incidentes; os processos de software e *DevOps* verificando explicitamente a integridade da segurança de aplicativos e *softwares* usando testes externos; o aumento da eficiência no gerenciamento da postura de segurança ao

simplificar a sua complexidade; e a adaptação e a expansão do *Zero Trust*, para resolver a escassez de competências em TI, a capacidade do pessoal e reforçar a postura de segurança (MICROSOFT, 2021).

5 CONSIDERAÇÕES FINAIS

Ao analisar os casos de boas práticas apresentados, alinhados com os princípios teóricos e conceitos da arquitetura *Zero Trust* entende-se que, ao aderir aos princípios fundamentais da ZTA, as organizações podem estabelecer uma estrutura de segurança robusta frente ao cenário de ameaças dinâmico e em evolução.

Vale ressaltar que a implementação destes princípios requer uma abordagem abrangente que combine tecnologia, processos e pessoas para alcançar uma confiança zero, além da mentalidade aberta para se construir uma postura de segurança resiliente.

Por ser um modelo que traz um novo paradigma para a segurança, para a visão e a cultura organizacional, alguns desafios podem se fazem presentes ao implementá-lo, como a dificuldade de compreensão das estratégias *Zero Trust*, sendo fundamental clareza na comunicação com as partes interessadas e sinergia com as necessidades do negócio.

O custo de implementação pode ser outro desafio, principalmente quando envolvem empresas de pequeno e médio porte que, mesmo em soluções aplicadas a uma infraestrutura mais simples e reduzida, torna-se inviável com menor orçamento.

Outros fatores que desafiam a sua implementação dizem respeito aos impedimentos ou mudanças que podem ocorrer mesmo com uma compreensão clara da estratégia, durante o processo, como a falta de fornecedores que possam entregar uma solução completa da arquitetura.

Nesse sentido, deve-se considerar que ao adotar o modelo *Zero Trust* é preciso analisar quais soluções ofertadas no mercado abrangem toda a estrutura, e caso não possua alguns componentes, que estes possam ser integrados a soluções de terceiros sem impactar negativamente desempenho e custos.

Contudo é necessário também atentar-se a essas soluções que atuam somente em partes específicas (gerenciamento da nuvem, gerenciamento de identidade, análise de transações etc.). A adição de ferramentas diversas para uma só arquitetura pode gerar uma complexidade na infraestrutura que irá dificultar o gerenciamento, o que diverge do modelo ideal.

É indispensável, portanto, que ao se pensar em soluções para implantação da arquitetura *Zero Trust*, que agreguem em um só sistema todos os ativos da empresa e o gerenciamento de toda a rede, para que deste modo haja simplicidade nos processos e otimização quanto ao gerenciamento de riscos de segurança da informação.

REFERÊNCIAS

ARRUDA, L. G. S. de; GIOZZA, W. F.; NZE, G. D. A.; NUNES, R. R. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. In: **Revista Ibérica de Sistemas e Tecnologias de Informação**. Publicado em junho de 2023. Disponível em:

https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf

Acesso em: 07 de setembro 2023.

FORTINET. **Fortinet relata que a América Latina foi alvo de mais de 360 bilhões de tentativas de ataques cibernéticos em 2022.** Publicado em fevereiro de 2023. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent. Acesso em: 07 de outubro 2023.

GIL, A. C. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas,1999.

GOODEN, G. **AWS perspective guidance: embracing zero trust:** a strategy for secure and agile business transformation. Amazon Web Services Inc., 2023. Disponível em: https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/strategy-zero-trust-architecture/strategy-zero-trust-architecture.pdf. Acesso em: 01 de outubro 2023

GOOGLE. **BeyondCorp Enterprise.** Google, 2022. Disponível em**:** https://cloud.google.com/beyondcorp-enterprise?hl=pt-br. Acesso em: 03 de outubro 2023.

_____. **Implementing zero trust security with chrome enterprise and beyondcorp enterprise**. Disponível em: https://services.google.com/fh/files/misc/chrome_enterprise_and_beyondcorp_enterprise_technical_paper.pdf. Acesso em: 04 de outubro 2023.

MALHOTRA, N. **Pesquisa de marketing**. Porto Alegre: Bookman, 2001.

MARCONI, M.A.; LAKATOS. E.M. **Fundamentos da metodologia científica.** São Paulo: Atlas, 2003.

MICROSOFT. **Envolving zero trust:** how real-world deployments and attacks are shaping the future of zero trust strategies. Microsoft Co., 2021. Disponível em: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT. Acesso em: 05 de outubro 2023.

PECK, J.; Beyer, B.; BESKE, C.; SALTONSTALL, M. Migrating to BeyondCorp: maintaining productivity while improving security. In: **Login**, vol. 42, nº 2, 2017. Disponível em https://www.usenix.org/publications/login/summer2017/peck. Acesso em: 04 de outubro 2023.

ROSE, S., BORCHERT, O., MITCHELL, S., & CONNELLY, S. Zero Trust Architecture. In: **Encyclopedia of Cryptography, Security and Privacy**. Springer Berlin Heidelberg: Stafford, 2020. Disponível em: https://doi.org/10.6028/NIST.SP.800-207. Acesso em: 14 de setembro 2023.

SEQUEIRA, J. **O paradoxo do Zero Trust: porque 60% das empresas têm dificuldades em maximizar os seus benefícios.** Publicado em 24 de fevereiro de 2023. Disponível em: https://www.computerworld.com.pt/2023/02/24/o-paradoxo-do-zero-trust-porque-60-das-empresas-tem-dificuldades-em-maximizar-os-seus-beneficios. Acesso em: 08 de outubro 2023.

TEERAKANOK, S.; UEHARA, T.; INOMATA, A. **Migrating to zero trust achitecture:** reviews and challenges. Volume 2021. Hindawi, 2021. Disponível em: https://doi.org/10.1155/2021/9947347. Acesso em: 03 de outubro 2023.

WARD, R; BEYER, B. BeyondCorp: a new approach to enterprise security. In: **Login**, vol 39, nº 6. Publicado em dezembro 2014. Disponível em:

https://www.usenix.org/system/files/login/issues/login_dec14_online.pdf. Acesso em: 07 de outubro 2023.