EnGeTec em Revista | 07
ISSN 2965-9302
v. 1 | n. 7 | e304 | Agosto 2024

Integração de blockchain e modelo *zero trust* para a segurança de dados em redes corporativas

Vinicius Gadelha dos Santos[1]
vinicius.santos216@fatec.sp.gov.br

Walison Martins Vitorio[1]
walison.vitorio@fatec.sp.gov.br

Blockchain integration and zero trust model for data security in corporate networks

Integración de blockchain y modelo de confianza cero para la seguridad de los datos en las redes corporativas

Palavras-chave:
Redes Corporativas.
Blockchain.
Zero Trust.
Segurança de dados.

Keywords:
Corporate Networks.
Blockchain.
Zero Trust.
Data Security.

Palabras clave:
Redes empresariales.
blockchain.
Zero Trust.
seguridad de datos.

Enviado em:
25 outubro, 2023

Apresentado em:
05 dezembro, 2023

Publicado em:
24 agosto, 2024

Evento:
6º EnGeTec

Local do evento:
Fatec Zona Leste

Avaliadores:
Edson Company Colalto Junior
Edson Saraiva de Almeida

Resumo:
A segurança e integridade de dados se torna cada vez mais prioridade no universo corporativo. Com a ascensão da blockchain, empresas vem adotando a tecnologia pelas suas características de segurança como a criptografia dos dados, imutabilidade e integridade das informações e sua descentralização de rede. Existem diversas estratégias e modelos de segurança de rede, contudo a combinação do modelo *zero trust* com redes blockchain tende a se provar eficiente e eficaz a aqueles que prezam pela segurança de seus dados. Busca-se revisar e analisar os conteúdos atualmente disponíveis através de uma abordagem qualitativa, ao qual se aplica o procedimento de pesquisa bibliográfica para validação do tema. O objetivo deste artigo é disseminar o conhecimento de novas tecnologias de segurança a fim de diminuir o risco de ataques a redes corporativas. Embasado em conceitos como não confiar em qualquer usuário ou dispositivo, o modelo *zero trust* adiciona uma camada de segurança ao qual integrada a redes blockchain pode ser uma solução eficaz para melhorar a segurança e transparência das redes corporativas.

Abstract:
Data security and integrity are becoming increasingly important in the corporate world. With the rise of blockchain, companies are adopting the technology for its security features such as data encryption, immutability and integrity of information, and its decentralized network. There are many different network security strategies and models, but the combination of the zero trust model with blockchain networks is likely to prove efficient and effective for those who want more security for their data. This article was made to review and analyze the contents currently available through a qualitative approach, to which the bibliographic research procedure is applied for validation of the theme. The purpose of this article is to disseminate the knowledge of new security technologies to reduce the risk of attacks on corporate networks. Based on concepts such as not trusting any user or device, the zero trust model adds a security layer that, when integrated with blockchain networks, can be an effective solution to improve the security and transparency of corporate networks.

Resumen:
La seguridad y la integridad de los datos se están convirtiendo cada vez más en una prioridad en el universo corporativo. Con el auge de la cadena de bloques, las empresas han adoptado la tecnología por sus características de seguridad, como el cifrado de datos, la inmutabilidad y la integridad de la información, y su descentralización de la red. Existen varias estrategias y modelos de seguridad de red, sin embargo, la combinación del modelo de confianza cero con las redes *blockchain* tiende a resultar eficiente y efectiva para aquellos que valoran la seguridad de sus datos. Se busca revisar y analizar los contenidos disponibles en la actualidad a través de un enfoque cualitativo, al cual se le aplica el procedimiento de investigación bibliográfica para validar el tema. El objetivo de este artículo es difundir el conocimiento de las nuevas tecnologías de seguridad con el fin de reducir el riesgo de ataques a las redes corporativas. Basado en conceptos como el de no confiar en ningún usuario o dispositivo, el modelo de confianza cero añade una capa de seguridad a la que las redes *blockchain* integradas pueden ser una solución eficaz para mejorar la seguridad y la transparencia de las redes corporativas.

[1] Faculdade de Tecnologia da Zona Leste

EnGeTec em Revista | 07
ISSN 2965-9302
v. 1 | n. 7 | e304 | Agosto 2024

1. Introdução

Com o constante aumento de ataques cibernéticos, empresas se viram no cenário de investir mais em segurança da informação para tentar amenizar os impactos negativos causado pelos ataques e ajudar a identificar falhas em suas aplicações (4INFRA, 2023). Tendências foram apontadas pelo 4INFRA (2023) em relação a como melhorar a segurança cibernética corporativa, visando aumentar a proteção de rede dos negócios. Dentre elas se destacam: A adequação da Lei Geral de proteção de Dados (Diretrizes para aumentar a segurança de dados e privacidade dos cidadãos), o uso de machine learning (aprendizado de máquina) e a implementação do modelo *zero trust* (confiança zero), ao qual se fundamenta na estratégia de proteger os dados críticos e sensíveis da corporação.

Criar uma rede blockchain é uma escolha provável por parte das empresas pensando em segurança cibernética (OKABAYASHI, 2022). Devido suas características de descentralização e criptografia das informações trafegadas, serviços críticos podem se beneficiar dessa arquitetura. Diversos modelos de segurança podem se integrar a rede blockchain para garantir a prevenção de ataques de invasão e vazamento de dados.

Neste contexto, este estudo tem como objetivo explorar os princípios do modelo *zero trust* e analisar como uma rede blockchain pode aplicar estes conceitos buscando aumentar a eficácia da segurança de sua rede.

2. Fundamentação Teórica

As organizações estão sempre em busca de novas maneiras de proteger seus ativos de ameaças cibernéticas, inclusive aplicando mais de um recurso de segurança em suas redes e recursos. Os modelos de segurança tradicionais são uma abordagem que tem sido usada por décadas, mas estão se tornando cada vez mais obsoletos. De acordo com a revista anual do grupo Thales (2022), em sua coleta de dados em cima de 2800 representantes empresariais, não foi obtido um resultado satisfatório em que os modelos tradicionais fossem considerados para a implementação empresarial em seu comparativo de uso entre os modelos de segurança utilizados atualmente.

Esses modelos se baseiam na ideia de proteger os ativos de uma organização dentro de um perímetro seguro. O perímetro é definido por uma série de controles, como firewalls, antivírus e segurança de rede. Utilizar o modelo de segurança castelo exemplifica a utilização do perímetro de rede já que esse modelo se baseia na semelhança de um castelo medieval. O castelo era protegido por um fosso e muralhas, do mesmo jeito, a rede interna é protegida por um firewall, antivírus e outros dispositivos de segurança. No entanto existem limitações, sendo uma das delas a vulnerabilidade a ataques internos. Se um usuário interno mal-intencionado for capaz de superar as defesas do perímetro, ele terá acesso irrestrito à rede interna. Outra limitação é que o modelo de segurança castelo pode ser caro de implementar e complexo de se manter (CLOUDFLARE, 2023).

Os modelos tradicionais se concentram em bloquear ou liberar o endereço IP daqueles que devem ou não acessar os seus recursos para garantir que apenas usuários autorizados tenham acesso a informações sigilosas, garantir a integridade dos dados assegurando que as informações não sejam alteradas ou corrompidas sem autorização, e pôr fim garantir a disponibilidade para que as informações estejam disponíveis para os usuários autorizados quando necessário (KIME, 2023).

Dentre os modelos tradicionais, podemos destacar os métodos de arquivos *blacklist* e *whitelist*. O arquivo *blacklist* é responsável pela segurança de rede da empresa, sendo capaz de bloquear requisições disparadas por determinado IP. Porém, inserir IPs manualmente tende a ser demorado e trabalhoso considerando o tempo para identificação do IP do invasor e o que ele pode fazer enquanto é detectado e inserido na *blacklist*, além do tempo de atualização do sistema para detectar a alteração no arquivo (KIME, 2023).

DOI: https://doi.org/10.5281/zenodo.13324038
Santos e Vitório (2024)
EnGeTec em Revista | 07
ISSN 2965-9302
v. 1 | n. 7 | e304 | Agosto 2024

Consequentemente, uma opção utilizada junto a *blacklist* é a *whitelist*. No arquivo de *whitelist*, serão inseridos os IPs que serão permitidos na aplicação, negando assim todos os acessos de endereços que não se encontram no arquivo. Neste caso, bastaria definir os IPs que teriam acesso a aplicação e autorizá-lo na rede (KIME, 2023). Com esse conjunto de arquivos, a segurança tradicional dificultava o acesso de invasores através de máquinas virtuais ou VPNs.

2.1. DESVANTAGENS DOS MODELOS TRADICIONAIS

Apesar de existir diversos modelos de segurança, sempre haverá alguma fresta que poderá ser explorada por um invasor, mas de acordo com cada modelo, o invasor deverá se adaptar na forma de navegação em que a implementação falha. Assim como o modelo castelo, o modelo de confiança implícita baseia-se na ideia de que os usuários e dispositivos dentro do perímetro de segurança são confiáveis. O acesso a recursos e sistemas é outorgado com base nas credenciais do usuário ou do dispositivo (CLOUDFLARE, 2023). Este modelo pressupõe que os usuários e dispositivos dentro do perímetro de segurança foram autenticados e autorizados. No entanto, esta suposição pode ser violada se o usuário ou dispositivo for comprometido. Ataques que utilizam credenciais comprometidas ou dispositivos infectados podem ocorrer, existe a possibilidade de um invasor roubar credenciais ou instalar malware no dispositivo para obter acesso à rede da organização. Sua utilização pode ser realizada em conjunto com outras políticas de segurança dependendo da criticidade do vazamento dos dados. Mesmo em uma rede interna, proteções como o bloqueio de acessos podem ocorrer por parte do time de segurança, com o uso de arquivos de *blacklist* e *whitelist*.

Com a variedade de recursos de segurança disponíveis e com diferentes propósitos, uma opção é a combinação de modelos de segurança para aumentar a proteção de suas redes e mais de um serviço de nuvem para armazenamento de dados. Esse tipo de abordagem tem tomado forma desde a pandemia de 2020. (THALES, 2022). No entanto, é importante considerar alguns aspectos ao implementar mais de um modelo de segurança. Deve se pensar em uma estratégia ao integrar diferentes modelos, sua integração tem que ser realizada de forma a fornecer uma proteção holística para a rede. Se os diferentes modelos de segurança não forem integrados de forma adequada, eles podem gerar conflitos ou ineficiências, além de altos custos e elevada complexidade caso a cadeia de modelos se sobrepor.

Os modelos de *blacklist* e *whitelist* citados anteriormente, tem as suas desvantagens sendo cobertas pelas vantagens da outra, e por isso são muito utilizadas em conjunto. Mesmo assim, um problema em comum traz um enorme risco a integridade dos dados da organização. Tratando-se da *blacklist*, ela tende a ser menos segura que uma *whitelist*, uma vez que será permitido o acesso do invasor a aplicações não autorizadas (KIME, 2023). Mesmo com uma grande massa de IPs no arquivo de *blacklist*, um ataque de engenharia social tornaria o método totalmente ineficaz. Já a *whitelist*, por sua vez, é desvantajosa por conta do seu gerenciamento, onde deve sempre estar atualizado com as aplicações que deverão ter acesso aos recursos que estarão protegidos (KIME, 2023).

Assim como a *blacklist*, a *whitelist* também seria ineficaz considerando um ataque de engenharia social, visto que um colaborador pode estar com seu IP no arquivo de *whitelist*, porém pode ter seu dispositivo comprometido pelo invasor. De modo geral, os dois arquivos pecam no quesito de usabilidade, tendo como principal desvantagem a atualização manual dos arquivos, onde o invasor poderá ter tempo o suficiente para obter os dados desejados até que o seu acesso seja finalmente barrado pela aplicação.

2.2. COMPARATIVO DE MODELOS TRADICIONAIS E MODELOS ATUAIS

Para esse comparativo, usaremos os conceitos de *blacklist* e *whitelist*, como modelos tradicionais. Para os modelos atuais, usaremos o conceito e aplicação de VPNs nas redes corporativas, sendo o modelo mais utilizado atualmente (THALES, 2022).

A princípio, a VPN traz uma vantagem ao se comparar com o modelo tradicional, uma vez que a configuração de uma VPN criptografa tuneis de rede para acesso aos recursos internos da organização,

DOI: https://doi.org/10.5281/zenodo.13324038
Santos e Vitório (2024)
EnGeTec em Revista | 07
ISSN 2965-9302
v. 1 | n. 7 | e304 | Agosto 2024

ao invés de permitir ou bloquear os IPs dos colaboradores. Ao utilizar recursos na nuvem, será possível obter os IPs que serão utilizados no acesso as aplicações, e para autorizar os usuários bastaria definir a permissão de acesso aos IPs configurados na nuvem, diminuindo assim riscos externos. Todavia, continuamos com a desvantagem de ataques de engenharia social, uma vez que, ao ter acesso ao arquivo de VPN de um usuário, o invasor teria acesso total a rede (GOSS, 2022).

Baseado na comparação dos modelos, temos vantagens na utilização de VPNs se comparada ao uso de *blacklist* e *whitelist*, porém seu desempenho pode ser um problema. De acordo com a *Cloudflare* (2023), a depender da configuração, a rota de internet utilizada até o servidor fará um caminho que trará muitos gargalos e lentidão ao usuário que está acessando alguma aplicação dependente deste arquivo. O modelo *zero trust* é um dos modelos atuais que melhor se enquadram na infraestrutura de rede de TI na atualidade, isso porque não haveria problemas de gargalos e mal desempenho como a VPN, além da sua redução de superfície de ataque de invasores pela sua característica de microssegmentação (CLOUDFLARE, 2023). Sua implementação de 2FA (Autenticação de dois fatores), reduziria também o risco de ataques de engenharia social considerando que os dados do colaborador estejam comprometidos, devido a necessidade de autorização em um segundo dispositivo.

2.3. O MODELO ZERO TRUST

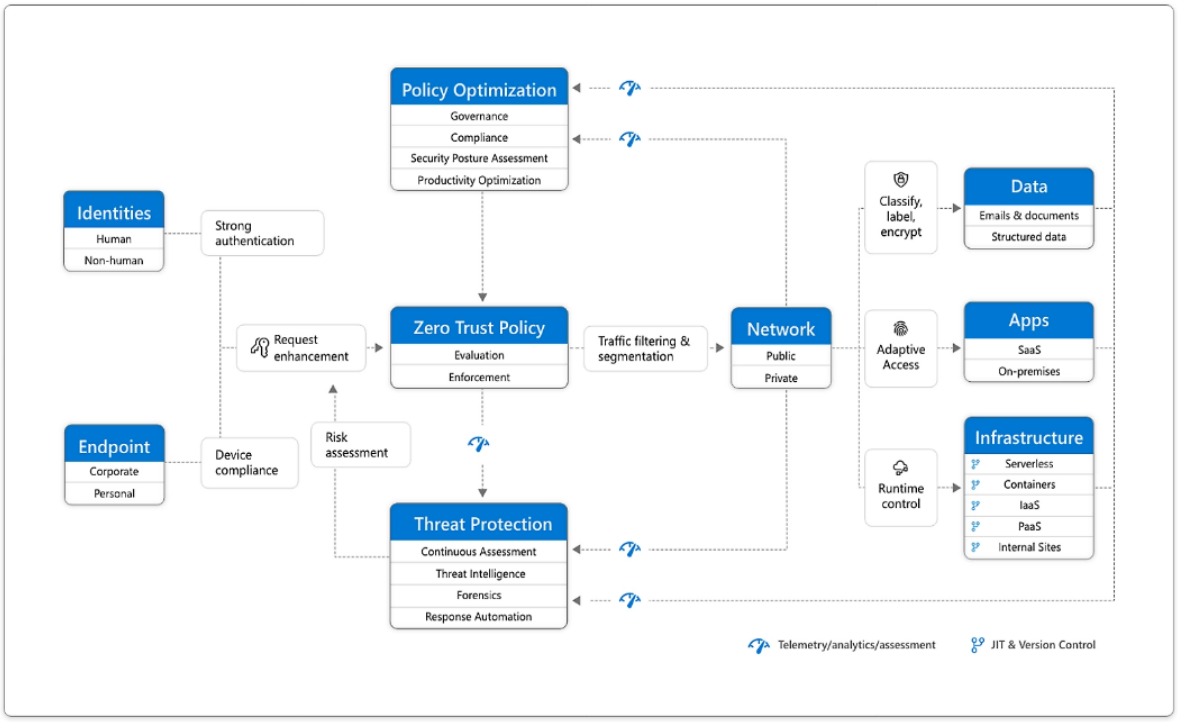
O *zero trust* conta com a premissa de que o risco está dentro e fora da organização, então nada na rede é confiável por padrão (GOSS, 2022). Diferente do modelo castelo, onde uma vez que o usuário for autenticado, ele terá acesso livremente a rede interna da organização, o modelo *zero trust* preza por desconfiar e verificar todo e qualquer tipo de requisição realizada por este usuário. Dentro da filosofia *zero trust*, até mesmo o usuário já autenticado será verificado rigorosamente enquanto navega pela rede interna, com acesso limitado aos recursos que ele necessita para executar o seu trabalho (APPS, 2022). Em uma arquitetura *zero trust*, o gerenciamento de acesso é monitorado constantemente, desde a solicitação de autorização até os seguintes passos que o usuário realiza. O modelo é definido por princípios fundamentais dos quais podem ser aplicados independentemente da arquitetura de rede escolhida (APPS, 2022):

- Acessos com privilégios mínimos - os usuários terão acesso somente ao que for necessário para a sua função, oferecendo assim mais segurança, impedindo que um usuário autenticado consiga navegar em um recurso em que não lhe foi concedido privilégios ou acesso.
- Autenticação multifator - cada usuário deverá ter no mínimo duas confirmações de identidade para que seja autenticado. Essas confirmações geralmente são compostas por uma senha de no mínimo 8 caracteres e uma confirmação em algum aparelho celular ou utilização de um token via aplicativo ou e-mail.
- Microssegmentação - é a divisão de um perímetro de segurança em várias zonas pequenas. Na prática, uma rede com arquivos armazenados em um único data center utilizaria a microssegmentação para conter outras zonas separadas e seguras. Logo, um usuário que possui acesso a uma das zonas, não deveria contar acesso a outras por conta do seu privilégio.
- Controle de acesso do dispositivo - além do rigoroso controle dos usuários, todos os dispositivos deverão ser monitorados a fim de prevenir riscos.

Na figura 1, podemos entender como o modelo *zero trust* da *Microsoft* atua, iniciando o seu processo na identidade do usuário e na validação de privilégio do usuário no *endpoint* que será acessado. Após ser autenticado, o usuário passará por um rigoroso monitoramento, onde todas as suas requisições serão verificadas pela política do *zero trust* junto a otimização de política que será definida pela organização. Para cada requisição realizada, serão coletados dados de telemetria para avaliação de risco e, caso necessário, o bloqueio do acesso caso o usuário autenticado seja identificado como suspeito.

EnGeTec em Revista | 07
ISSN 2965-9302
v. 1 | n. 7 | e304 | Agosto 2024

Figura 1 – Diagrama de definição da estrutura *Zero Trust*



Fonte: microsoft.com/en-us/security/business/zero-trust (2023)

Existem diversas vantagens ao se utilizar o modelo *zero trust*, contudo, sua implementação passa a se tornar um desafio para empresas que devem manter o modelo tradicional enquanto migra para o modelo *zero trust* pelo fato de que cada utilizador, dispositivo e aplicação deverão ser monitorados e reorganizados sob as novas políticas de acesso.

2.4. APLICABILIDADE EM REDES CORPORATIVAS BLOCKCHAIN

A adoção da blockchain em redes corporativas é uma tendência que tem o potencial de aumentar significativamente a segurança de dados (GARTNER, 2018). A blockchain é uma tecnologia de registro distribuído que oferece uma camada adicional de segurança para os dados corporativos. Ela é fundada em um sistema de criptografia que garante a autenticidade e a integridade dos dados, tornando-os difíceis de serem alterados ou adulterados (SOARES, 2023).

A blockchain pode ser usada para armazenar, processar e gerenciar dados corporativos de forma segura e transparente. Ela pode ajudar a proteger os dados contra acessos não autorizados, fraudes, erros e principalmente os dados críticos. Em redes corporativas, os dados críticos são aqueles que são essenciais para o funcionamento da empresa. Eles podem incluir informações financeiras, registros médicos, dados de clientes ou propriedade intelectual. Esses dados são frequentemente alvo de ataques cibernéticos, pois podem ser usados para causar danos financeiros, danos à reputação ou até mesmo para roubar identidades (UPX, 2021).

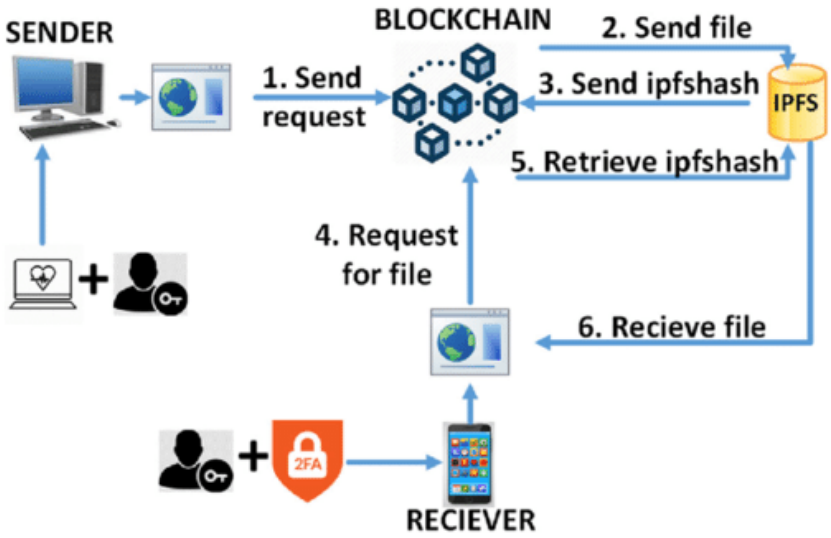
A Rede Record sofreu um ataque cibernético no dia 8 de outubro de 2022 (DIAS, 2022). Os hackers, que utilizaram o método *ransomware*, criptografaram os dados da emissora, impedindo o acesso a todo o acervo de reportagens, quadros e conteúdo já exibidos ou gravados. Parte do dano à emissora poderia ser mitigado se o compartilhamento dos dados em sua rede fosse em blockchain, pois os hackers teriam que criptografar cada bloco da blockchain para impedir o acesso aos dados. Isso seria muito mais difícil do que simplesmente criptografar um único arquivo ou servidor. Além disso, os hackers teriam que controlar mais de 50% da rede blockchain para modificar os dados. Isso é muito improvável, pois a rede ficaria distribuída em milhares de computadores. Não houve anúncios de

EnGeTec em Revista | 07
ISSN 2965-9302
v. 1 | n. 7 | e304 | Agosto 2024

planos de adotar a blockchain por parte da Rede Record, mas a tecnologia oferece uma série de benefícios de segurança que poderiam ajudar a emissora a se proteger contra-ataques cibernéticos.

Podemos integrar os conceitos de *zero trust* em redes blockchain para aumentar a eficácia da segurança conforme demonstrado na figura 2 (SULTANA et al., 2020). Os dados permanecem imutáveis, necessitando da validação dos blocos para assegurar a integridade da informação enquanto o *zero trust* toma a responsabilidade do acesso e autenticação utilizando 2FA (Autenticação multifator), assim aplicando o conceito de autenticação multifator e autorização com políticas definidas pelos administradores e organizadores da empresa.

Figura 2: Integração de princípios Zero Trust com Blockchain



Fonte: SULTANA et al. (2020)

Com uma ampla visão do tráfego de rede fornecida pelo *zero trust*, ferramentas de análise de risco podem ser utilizadas para identificar usuários ou dispositivos que representam risco maior para a segurança. Os administradores de rede controlam o acesso à rede com base no risco associado a cada usuário ou dispositivo. A identificação de atividades suspeitas como tentativas de acesso não autorizadas pode ser respondida rapidamente, ajudando a proteger os ativos mais valiosos da empresa. Essa abordagem de segurança acaba mitigando significativamente riscos que podem levar uma corporação a estados graves caso haja vazamento ou roubo de dados (APPS, 2022).

3. Materiais e Métodos

Usando o procedimento de pesquisa bibliográfica para o artigo corrente, foi analisado materiais já publicados, como artigos, internet, livros etc., com o intuito de utilizar uma abordagem qualitativa que de acordo com Coelho (2019), tem como objetivo central entender a explicação de algum fenômeno, através da interpretação dos dados.

Com base em análises do contexto atual das grandes corporações na era tecnológica, houve um aumento significativo nos ataques cibernéticos mundialmente. Nomeado como pandemia cibernética pela *Check Point Research*, foi ressaltado pelo grupo que houve um aumento de 50% nos ataques cibernéticos em todo o mundo em 2021, sendo 1 ataque a cada 61 organizações afetadas por *ransomware* a cada semana. Segundo o grupo, um dos maiores desafios enfrentados pelos profissionais de segurança são os ataques da Geração V, uma combinação ampla de ataques em grande escala e que por isso, é importante manter uma prevenção utilizando uma arquitetura de segurança capaz de barrar estes ataques.

EnGeTec em Revista | 07
ISSN 2965-9302
v. 1 | n. 7 | e304 | Agosto 2024

Já no Brasil, as estatísticas levantadas pelo grupo do *Check Point Research* este aumento sobe para 77% em comparação ao ano de 2021, sendo o principal mercado afetado pelos ataques as corporações de varejo e atacado com um aumento de 238%. Usando a rede Record como exemplo, em 2022 houve um ataque hacker a emissora do tipo *ransomware* onde informações e arquivos de reportagem, quadros e conteúdos já exibidos foram criptografados e exigidos 5 milhões de dólares para a recuperação dele.

Em contrapartida, foi analisado o aumento no interesse corporativo pela tecnologia blockchain. Conforme noticia a Bitcoin Magazine, segundo pesquisa global de blockchain de 2018 feita pela PwC, 84% dos executivos questionados dizem terem envolvimento com a tecnologia blockchain. No relatório, Gartner prevê que iniciativas com envolvimento na tecnologia gerarão cerca de 3 trilhões de dólares até 2030. O interesse em blockchain empresarial tem motivações, conforme afirma 101 blockchains, empresas necessitam de uma maior sofisticação em seu gerenciamento de dados e redes blockchain possibilitam maior segurança, transparência e menor complexidade e custo devido ser mais barato em comparação a outras abordagens tradicionais.

Fundamentado na necessidade da prevenção a ataques e aumento da segurança para manter integridade de dados corporativos, ao combinar a abordagem de jamais confiar e sempre verificar a origem e destino das informações trafegadas como ditada no modelo *zero trust* e redes descentralizadas como blockchain e seu aumento significativo na implementação por empresas, pode-se criar um ambiente seguro e robusto que se adapta ao constante crescimento de ameaças cibernéticas.

4. Resultados e Discussões

Conforme evidenciado, a preocupação com a segurança e integridade de dados é uma das prioridades para as empresas. Após a pandemia causada pela COVID-19, os profissionais de segurança mudaram sua forma de enxergar a segurança corporativa em meio ao contexto de trabalho remoto e o grande aumento de ataques hackers contra as companhias. Os impactos causados pela falta de preparo arquitetural na segurança de rede de uma companhia podem ser extremamente prejudiciais dependendo da criticidade em que os dados e informações tem ao negócio em que se atua. A escolha por modelos de segurança é de extrema importância ao querer prevenir ataques e ameaças, e mesmo que eficiente, sua má implementação pode ocasionar o inverso da proteção de seus dados. A abordagem citada pelo modelo *zero trust* se difere aos demais modelos pelo conceito de “nunca confiar, sempre verificar”, ou seja, dentro de uma arquitetura *zero trust* nenhuma entidade seja dentro ou fora da rede é inerentemente confiável, enquanto modelos tradicionais optam pela abordagem de “confiar, mas verificar” (BINOJ SS, 2023).

Vê-se que a ascensão da tecnologia blockchain devido as criptomoedas chama a atenção das grandes corporações desde 2018, devido as suas características de descentralização de rede e imutabilidade inerentes. Esse comportamento é devidamente fundamental quando se trata de segurança de rede. Devido a sua descentralização de rede, cada entidade recebe uma identidade criptografada única que tem como objetivo verificar e garantir a integridade dos dados também criptografados, assim, qualquer tentativa de alteração dos dados trafegados pela rede serão facilmente detectados pelas entidades que fazem parte da rede. Com sua natureza descentralizada, redes blockchain adicionam uma camada de segurança que dificulta o controle e manipulação das informações por usuários ou dispositivos suspeitos, enaltecendo a confiança dos dados armazenados e trafegados pelos blocos da rede.

Perante as informações coletadas, ao integrarmos o modelo *zero trust* com a tecnologia oferecida pela blockchain, pode-se construir uma solução promissora capaz de minimizar os ataques cibernéticos e garantir uma maior segurança a redes corporativas. Esta abordagem promissora tende a redefinir a maneira em que tratamos a segurança de dados do universo corporativo.

EnGeTec em Revista | 07
ISSN 2965-9302
v. 1 | n. 7 | e304 | Agosto 2024

5. Conclusão

Evidentemente, podemos notar a importância que se dá a segurança de redes corporativas em meio a um mundo cada vez mais tecnológico. Ataques cibernéticos causados pela falta de prevenção criam catástrofes capazes de causar prejuízos exorbitantes que podem encerrar o ciclo de vida de uma empresa. Apesar de não existir uma abordagem totalmente segura, a boa escolha e implementação de modelos de segurança podem garantir uma conexão segura entre entidades de rede.

Tecnologias inovadoras como a blockchain podem proporcionar alta escalabilidade e segurança devido suas características de descentralização de rede e criptografia de seus dados.

O atual estudo, através de pesquisas bibliográficas, teve como objetivo analisar e explorar como a integração de um modelo robusto de segurança como o *zero trus*t e uma rede descentralizada que garante a imutabilidade inerente de seus dados como a blockchain, pode ser uma solução promissora para a continua necessidade de evolução da segurança cibernética.

Enquanto ameaças virtuais continuam a aumentar, este trabalho espera incentivar o maior aprofundamento sobre a utilização de redes blockchain ao lado do modelo *zero trust* para garantir uma excelente prevenção a ataques de rede, além da busca por inovação de novos métodos de segurança.

Referências

O que é uma VPN?. **CLOUDFLARE**, 2023. Disponível em: https://www.cloudflare.com/pt-br/learning/access-management/what-is-a-vpn/. Acesso em: 16 novembro 2023.

Segurança de rede Castelo e Fosso. **CLOUDFLARE**, 2023. Disponível em: https://www.cloudflare.com/pt-br/learning/access-management/castle-and-moat-network-security/. Acesso em: 16 novembro 2023.

O que é uma rede Zero Trust? **CLOUDFLARE**, 2023. Disponivel em: https://www.cloudflare.com/pt-br/learning/security/glossary/what-is-zero-trust/. Acesso em: 15 novembro 2023.

THALES, **2022 Thales Data Threat Report**: Navigating Data Security in an Era of Hybrid Work, Ransomware and Accelerated Cloud Transformation, Global Edition, 2022. Disponível em: https://cpl.thalesgroup.com/sites/default/files/content/research_reports_white_papers/field_document/2022-03/2022-data-threat-report-global-edition.pdf. Acesso em: 16 novembro 2023.

THALES, **2022 Thales Data Threat Report**: Navigating Data Security in an Era of Hybrid Work, Ransomware and Accelerated Cloud Transformation, Emea Edition, 2022. Disponível em: https://www.exclusive-networks.com/se/wp-content/uploads/sites/25/2022/06/2022-thales-data-threat-report-emea-edition.pdf. Acesso em: 16 novembro 2023.

APPS, Spinning Cloud. Zero Trust Security: Everything You Need to Know. **Security Boulevard**, 2022.

Disponível em: https://securityboulevard.com/2022/11/zero-trust-security-everything-you-need-to-know/. Acesso em: 15 novembro 2023.

KIME, Chad. Whitelisting vs Blacklisting: How Are They Different? **eSecurity Planet**, 2023. Disponível em: https://www.esecurityplanet.com/applications/whitelisting-vs-blacklisting-which-is-better/. Acesso em: 15 novembro 2023.

GOSS, Michaela. VPN vs. zero trust vs. SDP: What's the difference? **TechTarget**. 2022. Disponível em:https://www.techtarget.com/searchnetworking/feature/SDP-vs-VPN-vs-zero-trust-networks-Whats-the-difference. Acesso em: 15 novembro 2023.

4INFRA. Tendências de segurança cibernética para 2023. **4INFRA**, 2023. Disponível em: https://4infra.com.br/tendencias-de-seguranca-cibernetica/#:~:text=Conhe%C3%A7a%20as%20tend%C3%AAncias%20de%20seguran%C3%A7a,padr%C3%A3o%20Zero%20Trust%20e%20computa%C3%A7%C3%A3o. Acesso em: 18 novembro 2023.

EnGeTec em Revista | 07
ISSN 2965-9302
v. 1 | n. 7 | e304 | Agosto 2024

BINOJ, SS. Enhancing Cybersecurity with Zero Trust and Blockchain Technology. **LinkedIn**, 2023. Disponível em: https://www.linkedin.com/pulse/enhancing-cybersecurity-zero-trust-blockchain-technology-s-s/. Acesso em: 18 novembro 2023.

OKABAYASHI, Mitie. Segurança de dados e Blockchain: entenda as relações. **Rípio**, 2022. Disponível em: https://launchpad-br.ripio.com/blog/seguranca-de-dados-e-blockchain-entenda-as-relacoes. Acesso em: 18 novembro 2023.

COELHO, Beatriz. Os diferentes tipos de pesquisa científica. Qual se aplica melhor a você? **Mettzer**, 2019. Disponível em: https://blog.mettzer.com/tipos-de-pesquisa/. Acesso em: 16 novembro 2023.

Guia de infraestrutura e proteção de rede. **UPX**, 2021. Disponível em: https://upx.com/post/infraestrutura-protecao-de-rede/. Acesso em: 15 novembro 2023.

MULLINS, Heath. Embrace proactive security with Zero Trust. **Microsoft**, 2023. Disponível em: https://www.microsoft.com/en-us/security/business/zero-trust. Acesso em: 17 novembro 2023.

DIAS, Gabriel. Record hackeada: entenda gravidade e como proteger os dados da sua empresa. **UOL**, 17 out 2022. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2022/10/17/ataque-hacker-record-roubo-de-dados-pode-ter-sido-um-dos-maiores-do-mundo.htm. Acesso em: 11 novembro 2023.

SULTANA, Maliha et al. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. **BMC Medical Informatics and Decision Making**, v. 23, n. 1, p. 5, 2020.

RESEARCH TEAM, Checkpoint. Check Point Research: Cyber Attacks Increased 50% Year over Year. **Check Point**, 2022. Disponível em: https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/. Acesso em: 15 novembro 2023.

HARPER, Colin. PWC GLOBAL SURVEY: CORPORATE INTEREST IN BLOCKCHAIN ON THE RISE. **Bitcoin Magazine**, 2018. Disponível em: https://bitcoinmagazine.com/business/pwc-global-survey-corporate-interest-blockchain-rise. Acesso em: 17 novembro 2023.

LAMOUNIER, Lucas. Blockchain Empresarial: A Transformação Industrial. **101 Blockchains**, 2019. Disponível em: https://101blockchains.com/pt/blockchains-empresarial/. Acesso em: 17 novembro 2023.

SOARES, Carlos S.S. et al. BLOCKCHAIN E SEGURANÇA DA INFORMAÇÃO-FORTRESS OF SECURITY. **Plural – Revista Acadêmica**, v. 2, n. 3, p. 3, 2023.