SOPHOS
Cybersecurity delivered.

Por que a ZTNA é importante: o futuro das redes seguras

ZTNA — proteção ao acesso remoto e defesa contra ransomwares

Documento técnico Sophos. Fevereiro de 2022

Quando se trata de segurança cibernética, tudo se resume em risco e confiança. Você confia no usuário que acabou de se conectar à sua rede, ou em quem está tentando acessar seus aplicativos corporativos? E aquele e-mail, que parece vir de um parceiro de negócios, mas que inclui solicitações um pouco incomuns que mais parecem um ataque de comprometimento de e-mail comercial? Na década de 1980, o slogan "Confie, mas confira" se popularizou, mas atualmente o pêndulo passou a oscilar para "Nunca confie. Confira sempre".

O modelo Zero Trust requer que todos na rede sejam autenticados para poderem ter acesso, mas isso não é tudo. Qualquer tentativa de acessar recursos na rede, como servidores, aplicativos ou dados, exige que o dispositivo ou aplicativo usado para acessar o recurso também seja validado para garantir a conformidade, e depois reautenticado e validado toda vez que uma nova solicitação é feita.

Da perspectiva da segurança cibernética, a confiança não se ganha, se conquista. Cada vez que um usuário, dispositivo e aplicativo partem para uma ação na rede, o processo de autenticação deve ser executado novamente.

O que é ZTNA?

O ZTNA (Zero Trust Network Access) se baseia no princípio do Zero Trust: "confie, mas confira", proporcionando segurança sensivelmente melhor ao tratar eficientemente cada usuário, dispositivo e aplicativo como seus próprios perímetros na microssegmentação da rede e avaliando e verificando constantemente a identidade e a integridade para obter acesso a aplicativos e dados corporativos. Os usuários têm acesso apenas a aplicativos e dados definidos explicitamente por suas políticas, reduzindo o movimento lateral e os riscos que o acompanham.

As vítimas de ransomware estão bem mais familiarizadas com a abordagem da conectividade ZTNA, provavelmente levadas pelo forte desejo de se prevenirem contra outros ataques. Trataremos sobre isso em detalhes mais adiante neste documento, quando falaremos sobre a visão dos usuários da Sophos e seu uso da tecnologia ZTNA.

A conectividade ZTNA é um componente fundamental na estrutura de segurança SASE (Secure Access Service Edge), que descreve como a segurança da rede e da nuvem se convergem em uma plataforma única entregue pela nuvem. O termo SASE, primeiramente descrito pela Gartner em 2019, é, essencialmente, a convergência do gerenciamento da tradicional rede WAN com as capacidades de segurança utilizando arquiteturas nativas na nuvem. Além do ZTNA, a arquitetura SASE inclui agentes de segurança para o acesso à nuvem, firewall como serviço, sistemas de prevenção contra invasões e gateways de acesso seguro.

O gerenciamento na nuvem oferece benefícios incríveis: instalação e utilização instantâneas, redução da infraestrutura de gerenciamento, implantação e registro, e permissão de acesso em qualquer lugar. Umas das maiores vantagens do gerenciamento na nuvem é a capacidade de fazer login imediatamente e começar a trabalhar, sem precisar de servidores de gerenciamento adicionais ou infraestrutura extra. O gerenciamento na nuvem também oferece o acesso instantâneo seguro em qualquer lugar e em qualquer dispositivo, para assegurar que você possa trabalhar do seu jeito. Também facilita o registro de novos usuários localizados em qualquer parte do mundo.

Contudo, a implementação ZTNA é um componente crucial para melhorar a segurança de usuários remotos e um significativo upgrade de segurança para os ambientes de rede voltados ao usuário remoto e impelidos pela pandemia, oferecendo também proteção da rede corporativa contra ataques de malware e ransomware.

Desconstruindo a ameaça à VPN

A pandemia teve um efeito devastador sobre a humanidade, mas trouxe um efeito benéfico inesperado de melhorar o acesso remoto: a implantação da ZTNA como substituto a uma VPN vulnerável. A pandemia forçou milhões de trabalhadores a atuarem fora do confinamento das redes corporativas mais "amigável" e a se estabelecerem no ambiente inóspito de seus lares, criando milhões de endpoints novos e vulneráveis, geralmente fora do controle das equipes de TI corporativas.

Esses endpoints são alvos oportunos para os invasores, pois, do ponto de vista estrutural, grande parte deles não apresenta as proteções que os endpoints empresariais costumam ter. Além disso, os milhões de usuários remotos recém-produzidos criaram uma imensa carga às VPNs corporativas que raramente tiveram que enfrentar tamanha carga de trabalho.

A conectividade ZTNA trabalha sob os princípios do Zero Trust para substituir as VPNs problemáticas, que são uma abordagem tradicional à conectividade de usuários remotos à rede corporativa. Tecnologicamente, as VPNs apresentam três grandes desvantagens para a extensa força de trabalho remota.

Primeiro, as VPNs não são projetadas para a escalabilidade e para atender à demanda das grandes empresas, que apresentam, comparativamente, um número substancial de funcionários remotos. Em segundo lugar, o software cliente da VPN, que costuma ser antigo, negligenciado e complicado, as torna alvos potenciais para os invasores. As VPNs também tendem a ter vulnerabilidades de segurança, pois foram criadas para usar a abordagem tradicional de segurança baseada em nome de usuário/senha. Por último, os usuários que acessam as redes usando VPNs acabam por, efetivamente, se conectarem como estações de trabalho executadas dentro dos perímetros de um firewall. Dependendo dos controles internos da rede, isso pode se tornar problemático.

Vamos analisar cada uma dessas questões e como a ZTNA as aborda.

As VPNs não são facilmente escaladas. Entre suas limitações estão a largura de banda das VPNs, que costuma se limitar a 1 Gbps, as portas expostas que podem ser usadas indevidamente, o potencial para ataques man-in-the-middle e o acesso privilegiado. Mais ainda, as VPNs são projetadas para lidar com um volume específico de usuários remotos e não podem ter sua capacidade de volume aumentada ou diminuída dinamicamente. Se o volume for muito alto, por exemplo, alguns usuários não serão capazes de acessar a VPN até que outros se desconectem.

Além disso, a Agência de Segurança Nacional dos EUA cita as vulnerabilidades da VPN em vários comunicados sobre segurança cibernética há anos e, em 2019, o Centro Canadense de Segurança Cibernética lançou diretrizes que observavam que três produtos de VPN populares apresentavam vários indicadores de comprometimento na detecção de atividades maliciosas. Esses indicadores incluíam redefinições de credenciais e vulnerabilidades dos protocolos SSL e TLS proprietários da VPN.

Por último, as VPNs não oferecem filtros quando conectam um usuário a uma rede. Basicamente, o usuário tem todos os privilégios como se fosse uma estação de trabalho por trás do firewall corporativo.

É possível reduzir a ameaça imposta pelas ferramentas de acesso remoto que dão ao invasor a capacidade de se movimentar pela rede de duas maneiras: Primeiro, exija que toda entrada na rede autentique o usuário, o dispositivo e o software a uma microssegmentação específica da rede. Mesmo que o invasor obtenha o acesso à rede, seus movimentos serão limitados. Em segundo lugar, restrinja de modo significativo os privilégios de todos à rede. Se o invasor não puder ver a rede por causa da limitação de privilégios, ele não poderá transpô-la.

O relatório The Forrester NewWave: Zero Trust Network Access, 3º trimestre, 2021, afirma: "Com a ZTNA, os usuários podem acessar aplicativos locais usando os princípios do Zero Trust, que, ao mesmo tempo, permite que o tráfego bidirecional de uma videoconferência siga diretamente para a Internet, melhorando assim a postura de segurança e a experiência do usuário". "Em síntese, a ZTNA reduz a necessidade de VPNs para os funcionários e abre caminho para as equipes de infraestrutura e segurança adotarem recursos de segurança e rede entregues pela nuvem."

O Zen da ZTNA

Da perspectiva da governança corporativa, gerenciar quem está na rede e o que estão fazendo está entre os pontos-chave de controle da empresa. Ter políticas e procedimentos que determinem como a empresa opera, e também ter práticas de negócios sólidas e éticas que levem à viabilidade financeira, são o propósito da função da governança corporativa. É possível, porém, que agentes nocivos fiquem na espreita, rondando a sua rede de maneira a comprometê-la ou para roubar dados confidenciais, instalar ransomwares e outros programas de malware, ou simplesmente aguardando furtivamente o momento mais oportuno para o ataque. Isso não apenas violaria as conformidades regulatórias e custaria à empresa altas somas em dinheiro, como também reduziria significativamente o valor de mercado da empresa.

Implantar um modelo de rede Zero Trust de modo geral e uma ZTNA de modo específico não apenas pode identificar invasores na rede, aplicativos malignos e benignos e usuários que não pertencem a ela, mas também reduzir significativamente a superfície de ataque de uma rede corporativa, melhorando ainda mais o perfil de risco geral da empresa.

Quando os usuários acessam a rede corporativa equipados com uma ZTNA, os dispositivos acessam os recursos da rede dentro de seus próprios perímetros microssegmentados, que são constantemente validados e verificados. Com o Zero Trust, os usuários não estão mais "na rede corporativa" em si, com toda a confiança e o acesso implícitos que normalmente os acompanhavam. Do contrário, eles têm acesso apenas às partes da rede para as quais eles e seus dispositivos tenham sido autenticados, o que não é o caso com as antigas conexões VPN.

Em uma rede tradicional em que os firewalls corporativos mantêm os invasores afastados, porém com poucas defesas em vigor após um usuário ter suas credenciais aceitas, os invasores podem se mover livremente em busca de credenciais mais elevadas que os permita ter acesso a áreas mais protegidas da rede para tentar roubar, copiar, corromper ou criptografar dados para pedir um resgate.

Implementar uma infraestrutura Zero Trust não apenas desmantela os esforços aplicados para o roubo de credenciais como também faz do firewall corporativo parte de uma estrutura maior do arsenal de defesa de dados e aplicativos. Mesmo que o computador utilizado por um funcionário que trabalha de casa seja infectado, as credenciais de usuário não serão suficientes para um ataque de peso depois que o invasor tiver acessado a rede corporativa.

Em verdade, a abordagem ZTNA dá acesso apenas limitado a parte da rede, pressupondo que o usuário terá as credenciais para se autenticar, autenticar seu dispositivo e também autenticar o software para utilizar um aplicativo ou dados para os quais tenha aprovação de uso.

Vencendo o ransomware

De acordo com o relatório da Sophos, O Estado do Ransomware 2021, 37% dos respondentes enfrentaram um ataque de ransomware no ano passado, e 54% deles disseram que os criminosos cibernéticos tiveram êxito na criptografia de seus dados. Olhando pelo prisma da perda de dados, a notícia não foi tão ruim assim, pois 96% dos respondentes disseram ter recuperado pelo menos parte dos dados. Porém, a parte negativa é que pagar o resgate raramente ajuda a reaver a totalidade dos dados: em média, apenas 65% dos dados criptografados foram recuperados após o pagamento do resgate.

Em 2020, a média de resgate pago pelas organizações de médio porte foi de US$ 170.404,00, como mostra o relatório. Porém, isso é apenas uma parte da conta total para remediar o problema. O custo médio para retificar o impacto do mais recente ataque de ransomware (incluindo o período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades, resgate pago e outros custos) foi de US$ 1,85 milhão, mais do que o dobro do custo relatado em 2020 de US$ 761.106,00.

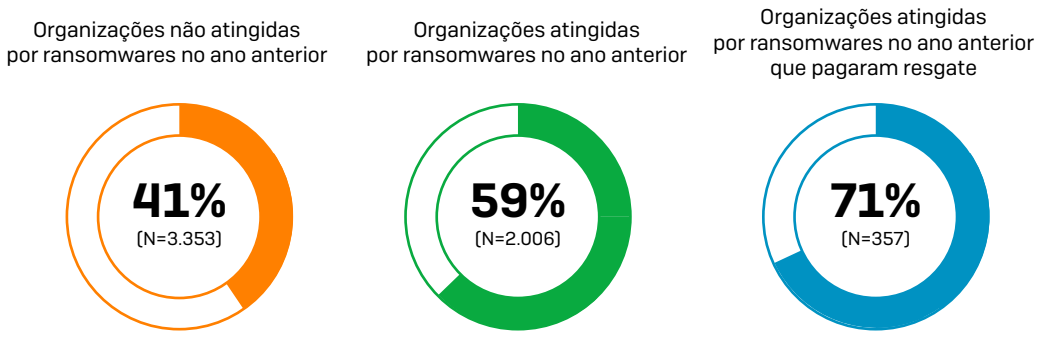
Em uma pesquisa recente com 5.400 profissionais de TI realizada mundialmente pela Vanson Bourne e apoiada pela Sophos, 20% dos respondentes disseram já ter implementado a abordagem Zero Trust, enquanto outros 41% afirmaram que já começaram a implementar o Zero Trust e esperam que tudo esteja concluído no início de 2022. Outros 20% esperam que tudo esteja finalizado no começo de 2023.

As soluções ZTNA eliminam um vetor comum de ataque por ransomware e outros ataques de infiltração na rede. Como os usuários da ZTNA não estão mais "na rede", mas em um microssegmento da rede corporativa, as ameaças que poderiam montar suas bases de operações através da VPN não têm para onde ir quando se trata de uma conexão por ZTNA.

Ataques de ransomwares levam à adoção da ZTNA

Resultados da pesquisa mostram que os profissionais de TI em organizações que foram atingidas por ransomwares no ano passado estão quase 50% mais propensos a estarem "bastante familiarizados" com a abordagem ZTNA do que aqueles cujas organizações não passaram por nenhum incidente (59% x 39%). Esse valor sobe para 71% entre as organizações que foram atingidas e que pagaram o resgate.

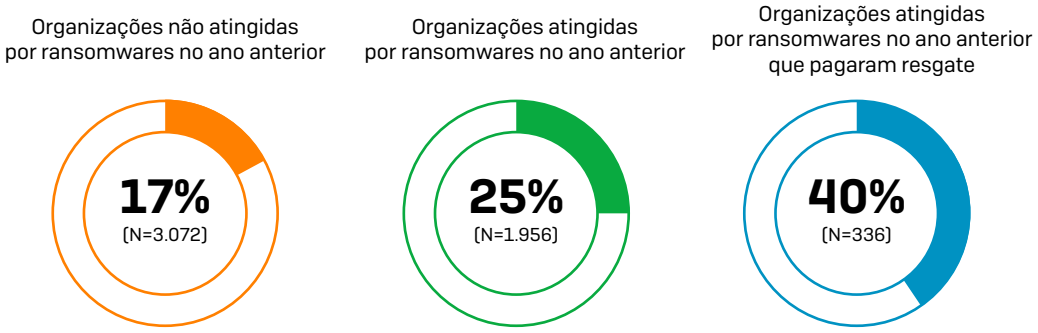
Porcentagem de respondentes que se consideram "Bastante familiarizados" com a abordagem Zero Trust Network Access (ZTNA)



Para ilustrar melhor esse ponto, apenas 10% das vítimas de ransomwares não estão familiarizadas ou têm muito pouco conhecimento sobre a ZTNA, em comparação com os 21% cujas organizações não foram vitimadas.

A pesquisa também mostrou que as vítimas de ransomwares estão mais à frente quando se trata de adotar o conceito Zero Trust. Um quarto (25%) dessas organizações que sofreram um ataque de ransomware no ano anterior já adotaram por completo uma abordagem Zero Trust, levando a um total de 40% entre as organizações que foram atingidas e que pagaram o resgate. Comparativamente, apenas um sexto (17%) das que não passaram por um ataque já migraram totalmente para essa abordagem de conectividade.

Porcentagem de respondentes cujas organizações já adotaram uma abordagem Zero Trust



As vítimas de ransomwares têm diferentes motivos para adotar a ZTNA.

- Os respondentes foram indagados sobre os motivos que os levaram a adotar uma abordagem Zero Trust e, ainda que tenha havido vários pontos comuns em suas respostas, as diferenças também foram notórias, com o motivador mais frequente entre as organizações atingidas e não atingidas sendo "Para melhorar nossa postura geral de segurança cibernética".
- O segundo motivador mais frequente entre as vítimas de ransomwares foi o desejo de "simplificar as operações de segurança cibernética" (43%), um possível reflexo de que a complexidade da segurança tenha contribuído para o ataque sofrido.
- As vítimas de ransomwares também estavam muito mais propensas a dizer que "mudar do modelo CAPEX para o OPEX" foi um dos principais fatores por trás da adoção de uma abordagem Zero Trust (27% x 16%, aumentando para 34% entre aquelas que foram atingidas por ransomwares e que pagaram o resgate).
- As vítimas de ransomwares também são altamente motivadas pelo "suporte à mudança e aumento do uso da nuvem" (42%), que caiu para 30% entre os que não passaram por um ataque recente.

Grandes expectativas

Pode ser difícil de explicar para a gerência ou os acionistas quais são os benefícios de um ambiente Zero Trust , pois não é fácil provar que um ataque foi malsucedido ou que simplesmente não aconteceu porque o invasor foi bloqueado antes que pudesse instalar um malware. Porém, é possível demonstrar que o Zero Trust reduz significativamente os riscos e que o risco reduzido pode ser monetizado pela empresa.

Reduzir o risco corporativo, por exemplo, pode levar a menores custos com o prêmio e melhores termos e condições do seguro de proteção digital, e, potencialmente, uma maior valorização da empresa. As seguradoras e corretoras de seguro de proteção digital reconhecem que baixos riscos levam a menos sinistros, resultando em menores pagamentos. A consequência é que a indústria do seguro de proteção digital está atualmente reavaliando e modificando seus termos na preparação de tais políticas, oferecendo melhores condições para as empresas reduzirem seus riscos de maneira proativa.

Na Ordem Executiva Presidencial para Melhorar a Segurança Cibernética da Nação, decretada pelo Presidente Joseph Biden em maio de 2021, a nova disposição estabelece que o governo federal "deve adotar boas práticas de segurança [e] avançar na direção da Arquitetura Zero Trust...". A adoção de um modelo Zero Trust pelo maior empregador da nação ressalta o reconhecimento de que essa abordagem é vista como o caminho para a redução de riscos.

A Gartner concorda que o Zero Trust é o caminho para a segurança cibernética no futuro. "Tanto para as grandes empresas, que já trilharam parte dessa caminhada, como para as que acabaram de começar, a proteção de dados deve ter a mais alta prioridade", disse a empresa. De acordo com a Gartner, 82% das empresas planejam deixar que seus funcionários trabalhem remotamente por um certo tempo. "Conforme as empresas começam a incorporar os trabalhadores remotos em seus planos de longo prazo, a segurança se torna uma prioridade. Contudo, muitas empresas estão começando a se dar conta de que a abordagem tradicional à segurança não é adequada para uma força de trabalho nativa na nuvem", escreveu a Gartner.

A Forrester também concorda, observando que a Zero Trust protege os recursos em lugar de proteger a rede física. "Em sua forma mais simples, o modelo Zero Trust muda o foco dos vários tipos de autenticação e controles de acesso para os controles personalizados baseados no armazenamento de dados confidenciais, aplicativos, sistemas e redes", escreveu a Forrester. "Esses controles aproveitam identidades, ativam/desativam usuários e intermediam o acesso com base em funções definidas."

Se o futuro é o Zero Trust, tudo começa com o controle de quem está na rede, o que podem acessar e como podem fazer isso. Essa é a *razão de existir* do ZTNA e o motivo de ser indispensável para o futuro da segurança cibernética.

Saiba mais em
sophos.com/ztna

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

22-02-06 PTBR (MP)

SOPHOS