Whitepaper Verificar a Segurança de Confiança Zero

Contents

Introduction

Este documento descreve informações relacionadas ao Zero Trust e como ele pode ser usado para proteger a empresa.

Resumo executivo

Zero Trust representa um modelo que pressupõe que nenhum usuário, dispositivo ou aplicativo, seja fora ou dentro da rede, possa ser considerado seguro e que cada um deve ser validado antes de ter acesso permitido aos ativos da rede.

Esse conceito ganhou mais importância na virtualização e na rápida movimentação de recursos locais para nuvens públicas, privadas e híbridas.

O termo Zero Trust foi criado pela Forrester em 2010 com o lançamento do Relatório Zero Trust Network Architecture.

Éimportante entender que o Zero Trust deve começar como uma estratégia no nível empresarial para proteger interesses e iniciativas comerciais vitais.

Pilares de confiança zero

O que é Confiança Zero?

O Zero Trust é uma abordagem estratégica que abrange várias tecnologias para ajudar a alcançar uma segurança mais prática para a infraestrutura atual. É uma arquitetura de segurança e uma metodologia empresarial projetada para orquestrar com eficiência a combinação atual de tecnologias, práticas e políticas.

Ele representa uma evolução em nossa abordagem de segurança e oferece uma abordagem de solução abrangente, interoperável e holística que incorpora produtos e serviços de vários fornecedores.

O Zero Trust é baseado em muitas tecnologias estabelecidas, como segmentação de rede, autenticação multifator e controle de acesso à rede.

Por que o Zero Trust é importante?

A confiança zero ajuda a proteger a empresa contra usuários não autorizados, violações e ataques cibernéticos. Você pode verificar continuamente a identidade de usuários e dispositivos e permitir que eles tenham apenas as permissões necessárias para realizar seu trabalho para minimizar o risco de um evento de segurança.

A investigação de mercado mostrou que se espera que a dimensão do mercado mundial de segurança de confiança zero aumente de um valor estimado de 27 mil milhões de dólares em 2022 para cerca de 60 mil milhões de dólares até 2027/2028, a uma taxa de crescimento anual composta de cerca de 17 % nessa altura.

Motivos:

- Maior frequência de ataques cibernéticos com base no alvo
- Crescimento nas regulamentações de proteção de dados e segurança das informações
- Maior necessidade de reduzir os riscos empresariais e organizacionais
- Àmedida que mais serviços são migrados para a nuvem, a implantação de dados centralizados ultrapassa os limites dos dados e aumenta os riscos de segurança.

- A necessidade de confirmar a identidade do usuário em todo o processo de acesso e não apenas inicialmente

Um único ataque de ransomware custa US$ 5 milhões. Os criminosos cibernéticos não discriminam quando têm como alvo empresas.

Pesquisas recentes de CIO e CISO mostram que a Zero Trust é uma das cinco principais prioridades. Os CISOs dizem que uma mudança para o trabalho remoto, uma falta de mão de obra e um grande pico em ataques de segurança cibernética exigem que seus sistemas existentes na empresa sejam protegidos.

Modelo tradicional x zero trust

Ambientes tradicionais são aqueles em que a segurança foi adicionada após a criação do ambiente. Normalmente, são redes planas onde as defesas são criadas em torno da borda da rede para evitar ataques da Internet.

O Zero Trust é geralmente reconhecido para se concentrar na necessidade de proteger os sistemas e dados de uma organização em vários níveis com uma mistura de criptografia, protocolos de computador seguros, carga de trabalho dinâmica e autenticação e autorização em nível de dados, e não depende exclusivamente de um limite de rede externo.

A arquitetura tradicional de segurança centrada no perímetro é menos eficaz, pois as cargas de trabalho são cada vez mais fornecidas da nuvem e os endpoints móveis se tornam a norma para o acesso a aplicativos e dados.

Estrutura de arquitetura com confiança zero

Uma Estrutura de arquitetura com confiança zero lida com a restrição de acesso a sistemas, aplicativos e recursos de dados para os usuários e dispositivos que precisam especificamente de acesso e foram validados. Eles devem ser autenticados continuamente de acordo com sua identidade e postura de segurança para garantir a autorização adequada para que cada recurso forneça acesso.

A estrutura é fornecer um roteiro para migrar e implantar conceitos de segurança de confiança zero para um ambiente corporativo e é baseada na Publicação especial 800-207 do NIST.

Uma estrutura arquitetônica eficaz do Zero Trust coordena e integra esses sete componentes principais.

- As redes Zero Trust são uma característica importante de uma estratégia Zero Trust que se refere à capacidade de segmentar redes ou isolar ativos de rede e manter o controle das comunicações entre elas. Além disso, ele protege conexões confiáveis para estender o local de trabalho para uso remoto.
- A força de trabalho com confiança zero abrange métodos para limitar e aplicar o acesso do usuário, o que inclui tecnologias para autenticar usuários e monitorar e controlar continuamente seus privilégios de acesso. Esse acesso é protegido por tecnologias como DNS, autenticação multifator e criptografia de rede.
- A Zero Trust Devices aborda a necessidade de isolar, proteger e gerenciar todos os dispositivos conectados à rede, que cresceram com a inclusão da mobilidade e da Internet

das Coisas, para criar uma imensa vulnerabilidade para os invasores explorarem.
- As cargas de trabalho com confiança zero protegem as pilhas de aplicativos da frente para trás que executam processos de negócios críticos. Concentra-se em proteger o tráfego leste/oeste entre aplicativos, dados e serviços em um data center para proteger melhor os aplicativos essenciais.
- Os dados de confiança zero referem-se a metodologias para classificar e categorizar dados, combinadas com soluções de tecnologia para proteger e gerenciar dados, o que inclui criptografia de dados.
- A visibilidade e a análise se referem a tecnologias que fornecem a percepção para automação e orquestração e permitem que os administradores não apenas vejam, mas também entendam a atividade em seus ambientes, o que inclui a presença de ameaças em tempo real.
- A automação e a orquestração englobam ferramentas e tecnologias, como algoritmos de aprendizagem automática e inteligência artificial, para classificar automaticamente os ativos de rede e data center, e para sugerir e aplicar medidas, políticas e regras de segmentação e segurança para que sejam aplicadas automaticamente; portanto, reduza a carga sobre as equipes de segurança e acelere a mitigação de ataques.

Confiança zero e segmentação

Todos os recursos baseados em rede devem ser protegidos e segmentados com o princípio do menor privilégio. Isso é feito melhor por meio de um sistema de gerenciamento de ativos que controla as credenciais e o acesso para todos os fins.

A necessidade de segmentação com confiança zero inclui proteção da marca, superfície de ataque limitada, estabilidade de rede aprimorada e habilitação de implantação de serviço rápida.

Para ajudar a alcançar ainda mais a proteção para recursos individuais, a microssegmentação pode ser usada. Tags de grupo escaláveis (SGTs) podem ser usadas onde um valor de tag é inserido no quadro Ethernet para identificar exclusivamente um recurso. Além disso, os dispositivos de infraestrutura englobam switches inteligentes, roteadores ou firewalls de próxima geração que podem ser usados como dispositivos de gateway para proteger cada recurso.

Visibilidade, análise e automação

Éimportante ter visibilidade completa de todos os ativos da organização e de todas as atividades associadas a esses ativos. Essa é a base do Zero Trust.

Para fornecer decisões de confiança e políticas dinâmicas, é necessário um conjunto contínuo de análises. Nossa abordagem arquitetônica do Zero Trust concentra-se nos componentes lógicos essenciais de uma estratégia de SDN com um mecanismo de política e um administrador de política para formar um plano de controle para restringir o acesso aos recursos por meio de pontos de aplicação de política em um plano de dados.

Os recursos necessários para que a Zero Trust Architecture forneça maior contexto de rede, aprendizado e garantia para realizar com segurança sua missão:

- Microssegmentação granular do acesso a usuários, dispositivos, aplicativos, cargas de trabalho e dados.

- Aplicação de políticas de segurança em todos os lugares onde o trabalho é realizado, o que inclui LANs, WANs, data centers, nuvens e a borda da rede.
- Gerenciamento de identidade abrangente - para estender o gerenciamento de identidade e acesso para incluir as identidades de usuários, dispositivos, aplicativos, cargas de trabalho e dados que se tornam novos microperímetros através do acesso definido por software.
- Defesa integrada contra ameaças que aproveita a inteligência e os feeds de ameaças globais.
- Controle totalmente automatizado e ágil da rede da sua organização para funcionar com segurança na escala desejada, desempenho e confiabilidade necessária para atingir o objetivo.

Etapas para Zero Confiança

A chave para a segurança abrangente do Zero Trust é estender a segurança por todo o ambiente de rede, seja na LAN, no data center, na borda da nuvem ou na nuvem. A conformidade é, obviamente, obrigatória.

Essa segurança deve incluir visibilidade total do ambiente de rede da sua organização. Etapas importantes para o centro completo Zero Trust em torno de:

- Identificar dispositivos e dados confidenciais. Identificar e classificar dispositivos, dados confidenciais e cargas de trabalho.
- Entenda os fluxos dos seus dados confidenciais.
- Crie sua política de segmentação Zero Trust. Cada ativo baseado em rede deve ser protegido e segmentado adequadamente com o princípio de menos privilégio e rigorosamente aplicado, controles granulares para que os usuários tenham acesso apenas aos recursos necessários para executar seu trabalho.
- Implemente políticas e postura. Isso pode ser realizado com plataformas como Cisco DNAC ou ISE.
- Monitore continuamente o ambiente de confiança zero. Implemente análises de segurança para monitorar e analisar incidentes de segurança em tempo real e identificar rapidamente atividades mal-intencionadas. Inspecione e registre continuamente todo o tráfego interna e externamente.

Obtenha acesso confiável

Para obter segurança abrangente com Zero Trust, as empresas devem ampliar sua abordagem com Zero Trust para toda a sua força de trabalho, local de trabalho e cargas de trabalho.

- Força de trabalho com confiança zero - os usuários e dispositivos devem ser autenticados e autorizados, e o acesso e os privilégios são monitorados e controlados continuamente para proteger os recursos.
- Local de trabalho com confiança zero - o acesso deve ser controlado em todo o local de trabalho, o que inclui a nuvem e a borda.
- Cargas de trabalho com confiança zero - o controle de acesso granular deve ser aplicado em pilhas inteiras de aplicativos, que incluem contêineres, hipervisores e microsserviços na nuvem, bem como data centers de agências tradicionais.

A Cisco, uma líder reconhecida pela Forrester, é uma forte defensora da capacitação com o Zero Trust em toda a sua rede - no local e na nuvem. Você pode não apenas aproveitar sua infraestrutura de rede da Cisco como uma base fundamental da sua arquitetura Zero Trust, mas também pode aprender sobre outros recursos de segurança Cisco Zero Trust que podem ajudar sua empresa na jornada da Zero Trust.

Portfólio seguro da Cisco

Eles podem ser usados para criar uma estrutura Zero Trust bem-sucedida:

- Acesso seguro e sem atrito para usuários, dispositivos e aplicativos através do **Cisco Duo**
- Segurança de nuvem flexível através do **Cisco Umbrella**
- Inspeção inteligente de pacotes através do **Cisco Secure Firewall**
- Proteção avançada contra malware via **Secure Endpoint** (formalmente AMP)
- VPN e acesso remoto seguros através do **Cisco AnyConnect**
- Proteção holística da carga de trabalho através do **Cisco Tetration**
- Segmentação de rede protegida com o **Cisco Identity Services Engine** (ISE)
- Visibilidade e microssegmentação de aplicativos por meio da **Cisco Secure Workload**
- Plataforma de segurança integrada via **Cisco SecureX**
- Solução Unified SASE com assinatura como serviço via **Cisco+ Secure Connect**
- Orientação especializada do **Cisco Zero Trust Strategy Service**
- Suporte e serviços completos por meio de **serviços de consultoria, consultoria e solução**

Summary

Uma das maneiras mais simples de pensar sobre Zero Trust é "Nunca confiar E sempre verificar". Isso se aplica a todas as conexões de rede, todas as sessões e todas as solicitações de acesso a aplicativos, cargas de trabalho e dados críticos.

As estruturas de segurança de confiança zero criam defesas de microperímetro localizadas em torno de cada recurso na rede da organização. Se projetadas corretamente, as estruturas podem proteger os ativos independentemente de onde eles estejam localizados.

Uma maneira eficiente de reduzir o risco é controlar o acesso a dados privilegiados e compartilhados e adotar o princípio do privilégio mínimo. Esse modelo de segurança permite a orquestração por meio de APIs, bem como a integração com plataformas de automação de fluxo de trabalho que fornecem visibilidade para usuários e aplicativos.

Implementado com sucesso, o Zero Trust pode ajudar a garantir operações seguras e contínuas em todo o ambiente de tecnologia da informação de uma organização e resultar em acesso confiável contínuo a cargas de trabalho, aplicativos e dados críticos de uma organização, para aprimorar as missões da sua organização.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.