netskope

White Paper

Melhores Práticas de Zero Trust

RESUMO EXECUTIVO

Muitas pessoas acham que a transformação digital é apenas uma tendência passageira. Ela é uma ruptura econômica que impacta o ritmo das inovações e do desenvolvimento organizacional. As empresas querem permanecer relevantes, lançar produtos e serviços no mercado mais rapidamente, ser ágeis e ter a capacidade de se reinventar quando surgir a oportunidade certa.

O crescimento vertiginoso da computação na nuvem e a explosão de dispositivos móveis criaram um hábito que faz com que os usuários desejem acessar continuamente informações em qualquer lugar, de qualquer dispositivo e a qualquer momento.

Uma mentalidade antiga é um obstáculo para as empresas atuais. As empresas estão entrando no mercado com novos modelos de negócios, interagindo em milhares de relacionamentos com terceiros, o que acaba criando uma visão diferente de como devemos nos preparar para o futuro. Atualmente, a confiança é observadora, contextual e adaptativa, e não preto no branco (bloquear ou permitir) como no passado. Nenhuma entidade pode assumir uma confiança implícita, e os componentes usados para estabelecer a confiança precisam ser avaliados o tempo todo. Em última análise, é disso que se trata a confiança zero. Uma abordagem mais sistemática e segura para o acesso a informações.

O atual ecossistema de tecnologia legado está desaparecendo, e a abertura na forma de pensar é essencial. A transformação digital não pode acontecer da noite para o dia ou por conta própria. Ela requer segurança e transformação da TI como mecanismo de suporte. Precisamos repensar a maneira como fornecemos acesso seguro a informações com transparência, porque essa é a única coisa que mantém nossos usuários satisfeitos com elevada fidelidade.

Conceitos de zero trust, quando aplicados corretamente, podem proporcionar exatamente isso.

O crescimento vertiginoso da computação na nuvem e a explosão de dispositivos móveis criaram um hábito que faz com que os usuários desejem acessar continuamente informações em qualquer lugar, de qualquer dispositivo e a qualquer momento.

INTRODUÇÃO

O crescimento exponencial da computação em nuvem não apenas permitiu que as empresas consolidassem seus padrões de hospedagem e reinventassem a forma como chegam ao mercado, mas também acelerou a execução, o que as equipes de TI tradicionais não conseguiam fazer com as tecnologias legadas. Embora possamos resumir o passado como "arquitetura de redes baseada em perímetro", atualmente somos muito mais abertos e diversificados.

No entanto, a nuvem é "um facilitador de negócios", e expandiu o cenário de ameaças de maneiras que quase esquecemos. Essa tendência de "evolução na nuvem" mudou a forma como avaliamos a confiança no contexto de risco à empresa. Atualmente, a confiança é observadora, contextual e adaptativa, e não preto no branco (bloquear ou permitir) como no passado. Nenhuma entidade pode assumir uma confiança implícita, e os componentes usados para estabelecer a confiança devem ser constantemente avaliados. Em última análise, é disso que se trata a confiança zero. Uma abordagem mais sistemática e segura para garantir acesso a informações.

Apesar de muitas organizações conduzirem os resultados através de abordagens padronizadas em endpoints, os líderes de negócios estão, mais do que nunca, considerando os desejos dos usuários. Como resultado, o aspecto operacional desses dispositivos está se tornando mais difícil de gerenciar, pois a quantidade de tipos de dispositivos que precisam de suporte é bem maior. Outras empresas estão se afastando da manutenção e da operação de endpoints, em vez de permitirem que os usuários tragam qualquer tipo de endpoint para o ambiente de negócios, e se concentrando em garantir a segurança das informações.

Em última análise, o que as empresas querem é permitir que seus usuários sejam inovadores, produtivos, e estejam seguros e protegidos, independentemente do tipo de dispositivo que usam, a que horas estão trabalhando ou de onde estão trabalhando. Isso exige uma arquitetura e um modelo de negócios abertos. Zero trust se concentra em:

- Acesso seguro de recursos independentemente da localização da rede, do usuário ou do dispositivo
- Aplicar controles de acesso rigorosos e inspecionar, monitorar e registrar o tráfego da rede permanentemente

A confiança zero avalia continuamente todos os aspectos do comportamento da entidade durante uma conexão de rede e fornece controles de acesso adaptativos com base em parâmetros definidos e níveis aceitáveis de risco comercial.

Finalidade e escopo

O objetivo deste documento é fornecer uma compreensão dos principais componentes e das etapas de implementação dos conceitos pragmáticos de zero trust.

O escopo deste documento se concentra no acesso a recursos empresariais, análise comportamental e observações.

Público

Este documento destina-se a um público diversificado, incluindo arquitetos de segurança, sistemas e redes, bem como líderes de programas de segurança, responsáveis pelos aspectos técnicos de construção, operação e proteção de recursos e ativos corporativos. Embora orientado tecnicamente, ele pressupõe que os leitores terão uma compreensão básica de segurança, redes e sistemas de TI.

A confiança zero avalia continuamente todos os aspectos do comportamento da entidade durante uma conexão de rede e fornece controles de acesso adaptativos com base em parâmetros definidos e níveis aceitáveis de risco comercial.

PRINCÍPIOS

Princípios são regras e diretrizes gerais que devem ser compreensíveis, robustas, completas, independentes e não pretendem afirmar o óbvio. Eles informam e apóiam como uma organização se propõe a cumprir sua missão e são projetados para serem duradouros e raramente alterados. Cada princípio deve fazer uma declaração que auxilie o processo de tomada de decisão na empresa.

Aqui estão vários princípios de alto nível que fornecem orientação ao implementar uma estratégia de zero trust que todo arquiteto de sistemas precisa considerar:

- Todos na organização devem entender o **CONTEXTO** de negócios da empresa.
  - Os ativos da empresa (informações) devem ter a criticidade definida (normalmente derivada do Plano de Continuidade de Negócios e processo de negócios a que ele oferece suporte) e sensibilidade (geralmente adquirida pela política de classificação de informações da empresa e os requisitos de integridade necessários dos dados e do processo de negócios).
- **NÃO** deve haver confiança implícita entre entidades.
  - Todas as entidades devem ser continuamente verificadas e avaliadas em toda interação na rede.
- A confiança não é binária, mas sim um contínuo.
  - Existem diferentes níveis de confiança, dependendo do contexto de negócios e do apetite de risco aceitável.
- O acesso é concedido **APENAS** ao recurso corporativo individual.
  - **NÃO** há acesso à rede, mas apenas acesso a recursos (aplicações, serviços, etc.).
  - Evitar "zonas de confiança" e, em vez disso, usar sessões individuais.
- Pressupor que todas as redes são iguais
  - Pressupor a ideia de equalizar a intranet e a Internet.

Pressupostos

É imperativo entender que certas condições serão pressupostas, como:

- A organização está disposta e apta a fazer o que for necessário.
- A organização conta com o apoio da sua liderança.
- Os recursos necessários já existem ou serão alocados à organização.
- Os recursos tecnológicos estão disponíveis para a organização.

DERIVAÇÃO DO CONTEXTO

O uso de princípios zero trust representa uma abordagem holística e estratégica para a criação de um programa de segurança. Uma estratégia deve orientar a política que é aplicada com base em um contexto de negócios específico. É essencial entender que zero trust não é um paliativo ou um produto. A implementação deve começar com uma abordagem ampla, com a política se tornando mais detalhada à medida que as necessidades do usuário, os requisitos da empresa e o impacto nos negócios forem melhor compreendidos.

A metodologia tradicional de aplicar controles através do conceito "Permitir/Bloquear" não funcionará mais e deixará a organização significativamente exposta a riscos. As organizações devem usar uma lente de risco para avaliar qualquer tipo de acesso a recursos, e isso depende muito do contexto.

A qualidade do contexto é extraída de vários componentes que devem ser levados em consideração durante qualquer questionamento de sessão, antes da conexão ao destino final. Esses componentes são:

- Dados
- Identidade
- Endpoint
- Aplicação (recurso)
- Rede
- Visibilidade e análise
- Automação e orquestração

Avaliação contínua

A avaliação contínua desses componentes proporciona o contexto usado para um cálculo de aceitação de risco que orienta o conjunto de controles, influenciando a adaptação dinâmica das políticas antes ou durante o acesso aos recursos.

Dados

O negócio está sempre evoluindo, mas o ciclo de vida dos dados permanece o mesmo. Os dados são a alma de qualquer negócio e devem ser tratados dessa forma.

Embora muitas organizações evitem ou considerem complexo fazer uma classificação típica de seus dados, é fundamental se alinhar ao primeiro princípio de zero trust, "Compreender o contexto de negócios", e realizar as seguintes etapas:

- Compreensão dos dados
  - Descoberta (a empresa deve entender a localização dos dados)
  - Classificação (a empresa deve definir seu valor relativo e, em seguida, analisar, contextualizar e organizá-lo como tal)

  - Mapeamento para confidencialidade (derivado da sensibilidade), integridade (derivada da sensibilidade) e disponibilidade (derivada do BCP/processo crítico para os negócios)
    - » Se isso for desconhecido ou indeterminado, atribua essas categorias (confidencialidade, integridade e disponibilidade) a uma classificação padrão. Esses detalhes permitem que uma política seja aplicada na primeira instância, que pode ser posteriormente refinada ao longo do tempo.
  - Identificação dos proprietários de dados e dos guardiões de dados.
- Proteção de dados
  - Inspeção (inspecionar todos os dados, por exemplo, decodificação SSL)
  - Governança (definir regras e diretrizes)
  - Controle (aplicar conjuntos de controle técnico)

Identidade

Existem muitos usuários em qualquer organização, mas nenhum usuário é igual a outro. Todos exigem um nível de acesso a recursos específicos, e os controles associados devem ser aplicados adequadamente. É crucial seguir o gerenciamento completo do ciclo de vida de identidade, começando com provisionamento por meio de gerenciamento e governança até o desprovisionamento, quando essa identidade não for mais necessária. O desprovisionamento é uma etapa em que muitas organizações falham por falta de um processo adequado.

Evitar violações e corrupção de dados são os principais resultados derivados de uma boa governança de identidades e programas de gerenciamento de acesso. Se os usuários certos tiverem acesso adequado aos dados corretos nos momentos certos, o risco de violação e corrupção afetarem as operações e os clientes de uma empresa é minimizado. Os programas de governança de identidade e gerenciamento de acesso devem poder abordar:

- Gerenciamento de acesso
  - Mapeamento de perfis de usuários
  - Provisionamento, desprovisionamento e transferências
- Avaliação de credenciais
  - Autenticação e autorização
  - SSO e MFA
  - Acesso privilegiado
- Governança
  - Governança de acesso
  - Processo de solicitação e aprovação
  - Processos de reconciliação e erros

Endpoint

Os tempos mudaram desde que as organizações exigiam "apenas" dispositivos gerenciados pela empresa. Atualmente, os usuários demandam inúmeros dispositivos para fazer seus trabalhos, ou seja, muitas organizações começaram a aceitar BYOD (Bring Your Own Device). Um inventário saudável de dispositivos é essencial para um conjunto gerenciado de dispositivos, pois todos precisam ser identificados, isolados e protegidos por meio da implementação de controles baseados em políticas. No entanto, as empresas precisam fornecer acesso seguro aos recursos sem se limitarem apenas a dispositivos fornecidos pela empresa.

Introdução de dispositivos não confiáveis ou não gerenciados. Há uma necessidade cada vez maior de as empresas permitirem o acesso de terceiros, o que, por sua vez, resultará em acesso de endpoints não confiáveis, além do BYOD mencionado anteriormente.

Uma organização deve levar em consideração os endpoints (confiáveis ou não confiáveis/gerenciados ou não gerenciados) ao definir sua política de acesso de confiança zero. Esta também não é uma política padronizada, por isso, existe a necessidade de se entender o usuário e o contexto dos negócios. Em algumas situações, os dispositivos não gerenciados terão o mesmo acesso à aplicação (e, subsequentemente, aos dados) que os dispositivos gerenciados. Em outras, não. Veja mais sobre isso na seção sobre pontuação de risco.

Aplicação

Com a proliferação de aplicações e serviços na nuvem e em SaaS, os modelos operacionais e de negócios mudaram. Um dos aspectos essenciais da segurança é restringir o acesso a recursos, neste caso, às aplicações, a um mínimo. Aqui, a confiança zero se torna extremamente poderosa, pois os usuários não precisam mais se conectar a redes, mas, em vez disso, conectam-se a uma aplicação ou a um serviço específico utilizando sessões individuais isoladas.

Todas as organizações devem ter uma compreensão clara do seguinte a partir dos acordos de aplicação:

- Tipo de aplicação
- Modelo de hospedagem
- Confidencialidade, integridade e disponibilidade da aplicação (derivado dos dados que ela acessa, armazenados ou processados, ou processo de negócios a que ela fornece suporte)
- Fluxos de transação - upstream e downstream
- Requisitos de acesso de terceiros
- O resultado de uma avaliação de risco da aplicação

Rede

O perímetro legado está desaparecendo, a conectividade é onipresente e a segurança se tornou distribuída. É vital entender os fluxos de transações e as interações entre dois ou mais pontos. O isolamento da rede e a microssegmentação para segmentos mais localizados são algumas táticas para minimizar o movimento lateral, mas também permitem controles mais granulares do acesso aos recursos.

As equipes de rede já entendem a topologia, o fornecimento de conteúdo e a qualidade do serviço por meio de monitoramento e otimização de desempenho, mas zero trust introduz mudanças mais dinâmicas na arquitetura de rede onde são necessários ajustes.

Endpoints e usuários não acessam mais as redes. Ainda assim, eles têm conectividade direta com um serviço, uma aplicação ou uma carga de trabalho individual (este é o poder da confiança zero, pois agora podemos reduzir significativamente nossa superfície de ataque), portanto, é crucial aplicar os seguintes conceitos:

- Adotar a postura de segurança de "Negação padrão"
- Evitar "zonas de confiança"
- Isolamento de sessão
- Microssegmentação

Visibilidade e análise

É fundamental obter visibilidade das transações entre os componentes mencionados acima com detalhes contextuais e correlacioná-los e analisá-los. Como resultado, podemos entender melhor a interação, a qualidade e o desempenho de um ecossistema construído, para aprimorar e aplicar novas políticas refinadas e, assim, a adoção de controles. Os recursos devem estar alinhados a resultados e propósitos específicos, como melhorar a velocidade de detecção e resposta a ameaças onde a equipe de RI é o maior consumidor, com foco na localização de ameaças, investigação forense, atividades de conformidade etc.

Programas maduros de confiança zero devem ser capazes de:

- Inspecionar todo o tráfego (inspeção profunda de pacotes, além da telemetria de rede)
- Correlacionar dados entre fontes múltiplas e distintas com o gerenciamento de eventos e informações de segurança (SIEM)
- Identificar comportamentos anômalos com a análise do comportamento de usuários e entidades (UEBA)
- Fornecer uma visão holística do ambiente

Automação e orquestração

Atualmente, um dos desafios significativos para muitas organizações é a disponibilidade de recursos de qualidade. A segurança é uma das verticais mais impactadas, quando ocorre uma desvantagem na capacidade. Os indivíduos não podem fornecer velocidade e escala suficientes para lidar com essas complexidades no ecossistema. O aumento da complexidade exige o uso da automação.

A automação e a orquestração proporcionam uma capacidade incomparável de fornecer um programa de segurança mais eficiente. Tudo se resume ao processo certo no momento certo. Com a automação, as organizações podem acelerar a identificação e a resolução de ameaças específicas com um nível de precisão que os humanos não podem alcançar.

Pontuação de Riscos e Definição da Política de Acesso

A determinação do acesso a recursos, como aplicações, serviços ou dados, é gerenciada pela aplicação de controles definidos pelas políticas. Essas políticas impõem regras de acesso que são determinadas pelo apetite de risco da organização. A definição das políticas e, consequentemente, quais controles são aplicados, deve ser orientada por critérios que avaliam cada um dos componentes discutidos anteriormente.

As organizações podem adotar duas abordagens:

- Para cada atributo, avaliar cada cenário de implementação possível e definir uma regra que permitirá (ou restringirá) um nível de acesso e aplicá-los cumulativamente.
- Estabelecer um modelo de risco que aplique uma ponderação aos cenários de implementação de todos os atributos e definir as políticas de acesso com base no agregado dessa pontuação.

Por exemplo, para a abordagem um, no caso de dispositivos não gerenciados, a organização pode decidir que dispositivos não gerenciados só podem obter acesso a aplicações que processam, armazenam ou acessam dados com baixa classificação de confidencialidade e classificação de integridade. Além disso, o contexto do usuário pode ser incluído nesta decisão de política, por exemplo, um usuário interno proveniente de um dispositivo não gerenciado pode acessar aplicações que processam, armazenam ou acessam dados com classificação mais elevada de confidencialidade e de integridade. Ainda assim, eles não podem acessar aplicações ou dados mais críticos.

Cada permutação pode conduzir uma definição de política diferente, portanto, um conjunto de controles diferente é aplicado.

As permutações de amostra estão listadas a seguir, mas a organização precisa documentar e avaliar isso por conta própria para que elas se ajustem à forma como a organização opera e se alinhem aos seus padrões e práticas existentes:

- **Usuário:** funcionário interno, contratado interno, terceirizado
- **Classificação de confidencialidade de dados:** altamente confidencial, confidencial, privado, público
- **Classificação de integridade de dados:** muito alta, alta, média, baixa
- **Classificação de disponibilidade de dados:** altamente disponível, 0-4 horas, 4-24 horas, 24 horas
- **Endpoint:** gerenciado, não gerenciado
- **Aplicação:** crítica, importante, pequena

No que diz respeito ao conceito de avaliação contínua, ao longo de uma sessão de usuário, esses componentes devem ser avaliados e verificados o tempo todo. Se uma mudança for observada, é necessário tomar uma medida. Talvez encerrar a sessão, forçar a reautenticação ou executar uma autenticação de uma nova sessão.

Um exemplo pode ser que a sessão agora pareça ser originária de um dispositivo não gerenciado, quando anteriormente se pensava ser de um dispositivo gerenciado. Também pode ser que o usuário esteja agora tentando acessar dados com maior confidencialidade do que o que foi avaliado inicialmente.

CONCLUSÃO

A maioria das arquiteturas de segurança atuais foi desenvolvida para abordar um ecossistema de tecnologia que não é mais relevante. Uma nova forma de pensar é necessária para novas maneiras de operar e viabilizar seus negócios. A arquitetura de segurança deve se concentrar em entender claramente os riscos do negócio, seu contexto e aplicar controles adaptativos para enfrentar novos desafios, permitindo que usuários e empresas avancem rapidamente.

É imperativo implementar um equilíbrio adequado entre segurança, privacidade e experiência do usuário.

A Netskope, líder global em segurança cibernética, está redefinindo a segurança de nuvem, dados e rede para ajudar as organizações a aplicar os princípios de zero trust para proteger os dados. A plataforma Netskope Intelligent Security Service Edge (SSE) é rápida, fácil de usar e protege pessoas, dispositivos e dados em qualquer lugar. Saiba como a Netskope ajuda os clientes a estarem preparados para tudo, acesse netskope.com.