O New Trust Standard

Um paradigma para as relações de tecnologia confiáveis do futuro

Conteúdo

Resumo executivo

Seus clientes podem confiar os dados deles a você? Como eles podem saber?

A confiança costumava se resumir a um aperto de mão. Uma promessa de uma pessoa para outra. Mas os negócios se tornaram muito complexos para basear a confiança apenas em relacionamentos pessoais. A confiança do cliente depende da segurança e da transparência de toda a empresa: produtos, serviços, equipe, processos, ética e valores, sistemas internos, fornecedores e prestadores de serviços. A confiança do cliente depende não apenas das políticas, mas também dos seus fornecedores e dos fornecedores do fornecedor. Não apenas da sua segurança digital, mas também do que você faz quando uma violação ocorre. Não apenas sobre como você armazena dados privados dos clientes, mas também como você responde a uma solicitação da polícia estrangeira na sexta-feira à tarde.

Na economia digital atual, um parâmetro objetivo para avaliar a confiança é vital. Exige transparência total. Os dados que fluem pela Internet (às vezes na nuvem de um provedor) incluem dados confidenciais, como credenciais de login, números de identificação do governo, informações financeiras, segredos comerciais, planos de negócios e detalhes importantes de infraestrutura. Se as informações confidenciais forem para as mãos erradas, as consequências poderão incluir violações de privacidade, perda de propriedade intelectual, interrupções de operações e receita, blecautes e até ameaças à segurança nacional.

Chegou a hora de um New Trust Standard. É uma compilação do que ouvimos em conversas com milhares de clientes em todo o mundo, ao longo dos anos. O New Trust Standard é uma estrutura de expectativas e responsabilidade, em que as empresas e seus clientes podem concordar com novas regras para relacionamentos digitais confiáveis.

A confiança não tem nada a ver com criptografia, certificação ou supervisão da cadeia de fornecimento. Está relacionada a uma combinação de coisas. O que certamente mudará com o tempo, em resposta à evolução das expectativas dos clientes, da tecnologia, das ameaças digitais e da administração de dados internacional. Continue lendo para conhecer os principais elementos do New Trust Standard hoje.

Componentes essenciais do novo padrão de confiança

- **Afaste os invasores.** Filosofia Zero Trust
- **Gerencie o risco do fornecedor.** Cadeia de fornecimento confiável
- **Respeite os direitos dos dados.** Expectativas e regulamentações
- **Seja honesto sobre o que você faz.** Transparência
- **Prove.** Certificações e testes regulares de penetração

"Nossos clientes precisam de inovação mais do que nunca, mas também querem parceiros em que possam confiar."

Chuck Robbins
Presidente e CEO, Cisco

Evite invasores – filosofia “zero trust”

Verifique cada conexão, cada dispositivo, sempre

Seja cético, curioso, detalhista. Esses são os requisitos de trabalho para profissionais de segurança, porque a confiança começa com uma suspeita saudável. Como o nome indica, zero trust é uma filosofia de “nunca confiar, sempre verificar”.

Ao selecionar uma empresa, uma mentalidade zero trust significa questionar as práticas e políticas de segurança da empresa. O New Trust Standard diz que você tem o direito de solicitar, e de esperar, respostas claras. Se a empresa lida com dados confidenciais, uma mentalidade zero trust significa sempre questionar as suposições. Os clientes são o que dizem ser? Os dispositivos estão seguros? A aplicação A tem um motivo válido para conversar com a aplicação B?

A abordagem de décadas para controle de acesso e uma rede virtual privada (VPN) não se sustenta mais. Ela pressupõe que qualquer dispositivo que se conecte de dentro da rede corporativa pode ser confiável. E que quando um usuário e um dispositivo passam em um ponto de verificação, é seguro deixá-los se conectar a várias aplicações sem reautenticar. Hoje, nenhuma dessas suposições é verdadeira. Um laptop ou tablet pessoal usado para o trabalho pode ter sofrido uma infecção em casa. Um dispositivo que esteja limpo às 8h pode ser comprometido às 8h03 após um ataque de phishing. Com o armazenamento e o processamento de dados distribuídos na borda da rede, não há mais um alvo central para cercar. Além de autorizar conexões de dispositivos de usuário a servidores, as equipes de TI também precisam verificar se são permitidas conexões entre aplicações, dispositivos e sensores. Exemplo disso: algo que se parece com uma câmera de segurança não tem nada a ver com conectar-se a um banco de dados de clientes.

A abordagem moderna de controle de acesso é uma arquitetura zero trust. Ela trata todos os recursos como se fossem externos. Verifica a confiança antes de cada tentativa de acesso. E concede acesso apenas ao recurso necessário. Isso é verdade mesmo que o resultado venha do escritório do CEO. Mesmo que a postura de segurança do dispositivo tenha sido verificada há 30 segundos quando ele se conecta a uma aplicação diferente.

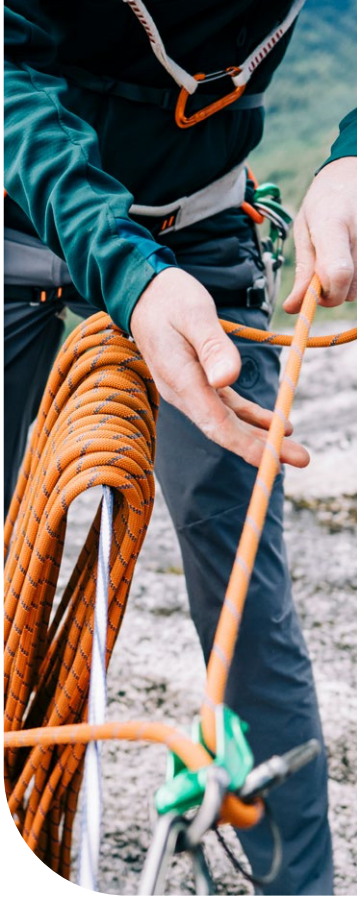
Princípios de zero trust

- Manter a experiência do cliente em mente. A autenticação não deve ser um fardo. Os usuários precisam ter acesso conveniente a aplicações na nuvem e no local para fazerem seu trabalho.
- Verificar continuamente se usuários, dispositivos e aplicações são confiáveis.
- Usar o aprendizado de máquina para identificar tentativas de login que se desviam do comportamento típico do usuário. Os falsos positivos acontecem, então considere os riscos de bloquear tentativas de acesso legítimas.
- Combinar a força da política de segurança da aplicação com a sensibilidade dos dados. Isso exige uma classificação precisa dos dados. Também requer uma compreensão da aparência do tráfego de aplicações normal para que os desvios possam ser detectados.
- Proteger conexões entre diferentes componentes de aplicações, como a lógica da aplicação e o banco de dados.
- Dificultar a movimentação de invasores que obtêm acesso a um servidor para outros servidores. As técnicas incluem segmentação de rede, autenticação e criptografia fortes e marcação de dispositivos confiáveis.

> *"A maioria dos provedores de nuvem já verifica a postura de segurança do dispositivo antes de conceder acesso. O New Trust Standard identifica imediatamente tentativas suspeitas que preveem resultados ruins e depois automatiza a resposta."*
>
> **Den Jones**
> Diretor sênior, segurança corporativa, Cisco

> *"Uma arquitetura zero trust é um grande investimento para entender e gerenciar melhor os riscos por meio de controles e restrições de administração, e para melhorar constantemente ao longo do tempo com aprendizagem de máquina."*
>
> **Brad Arkin**
> Vice-presidente sênior, diretor executivo de segurança e confiança, Cisco

Gerencie o risco do fornecedor



Confie na criação de uma cadeia de fornecimento confiável pelo fornecedor

Quando você compra um carro, confia no fabricante para tomar medidas razoáveis para avaliar a qualidade das peças do fornecedor, como freios e cintos de segurança. Da mesma forma, os clientes esperam que seus provedores de serviços conheçam todos os componentes de seus produtos e tomem medidas razoáveis para detectar e mitigar vulnerabilidades que possam levar à manipulação de dados, espionagem, interrupção e falsificação.

Não é fácil. Os provedores de serviços em nuvem normalmente usam software de terceiros para processamento de pagamento, autenticação, gerenciamento de dados e armazenamento, entre outros. Até mesmo o código proprietário geralmente inclui componentes de código aberto fornecidos por pessoas de todo o mundo, e muitos desses componentes têm vários componentes agrupados.

O que é “razoável” para os controles de fornecedores continua evoluindo. Os desencadeadores de mudanças incluem novos tipos de ameaças, novas práticas do setor e avanços de segurança digital.

Melhores práticas de cadeia de fornecimento

Defenda-se contra modificações. Execute um programa para garantir que as soluções com o seu nome sejam originais, operem conforme as instruções dos clientes e não sejam controladas ou acessíveis por terceiros.

Exija que os fornecedores sigam os padrões certos. Trabalhe com os fornecedores para avaliar, monitorar e melhorar suas práticas de segurança. Os padrões do setor são um bom ponto de partida. Os exemplos incluem NIST 800-53 para controles de segurança e privacidade, ISO/IEC 27001 para gerenciamento de segurança de informações, ISO 27018 para proteger informações de identificação pessoal (PII) em nuvens públicas e ISO 27701 para gerenciamento de informações de privacidade.

Estabeleça uma cadeia de confiança. O essencial é exigir que os fornecedores de software e hardware documentem a linhagem, ou proveniência, de seus produtos. Como um passaporte, esse registro mostra todos os lugares por onde o produto passou, desde o projeto e a construção até a fabricação e a entrega. Os fornecedores de software documentam onde o código foi criado, quem o assinou, os componentes usados para gerenciamento de identidade, onde o código foi compilado etc. Os fornecedores de hardware registram detalhes como o número de série de cada conjunto da placa de circuito impresso e quem o colocou na embalagem.

Incorpore confiança ao contrato. Responsabilize os fornecedores pelos mesmos padrões de segurança e privacidade que você se compromete a cumprir. Defina os requisitos para o teste e o relatório de vulnerabilidade. Inclua a linguagem no contrato para proteger os dados dos clientes após o término de um relacionamento com o fornecedor, por exemplo, ao exigir o retorno ou a destruição desses dados.

Teste as integrações com produtos próprios ou de outros fornecedores. Verifique se a integração não criou uma nova vulnerabilidade.

Realize auditorias regulares, incluindo testes de vulnerabilidade. Trabalhe com o fornecedor para criar um plano de identificação e correção de vulnerabilidades. Escreva o plano de resposta no contrato.

Respeite os direitos de dados

Fique à frente da evolução das expectativas dos clientes e das regulamentações governamentais

Os clientes esperam que os provedores mantenham seus dados protegidos e seguros, este é um requisito fundamental de confiança no mundo digital. Além disso, os clientes querem ser informados sobre como seus dados são coletados, usados e gerenciados e, por fim, os clientes querem o controle de seus dados. Esse desejo de visibilidade e controle abrange qualquer relacionamento de dados, de um indivíduo envolvido nas mídias sociais, um hospital armazenando registros médicos a uma empresa que usa serviços de colaboração na nuvem. Cada vez mais, os consumidores tomarão decisões sobre seus provedores com privacidade e transparência em mente.

Expectativas do cliente

Para confiar no provedor, os clientes geralmente querem garantia sobre estes pontos:

- Nosso conteúdo é nosso
- Está sujeito às mesmas leis que estamos
- É acessível somente para pessoas que autorizamos e esperamos

Os clientes dependem e, geralmente, estão sujeitos a regulamentações governamentais que visam proteger a privacidade. A administração internacional de dados[1] refere-se a leis globais coletivas, regulamentações e normas associadas à proteção de dados, à privacidade de dados, ao compartilhamento de dados e ao uso de dados. O New Trust Standard sustenta que os provedores de serviços devem ser transparentes quanto à sua abordagem de soberania de dados, ou seja, o conceito de que os dados estão sujeitos às leis do país em que são coletados. As leis de privacidade foram promulgadas em mais de 130 países que buscam estabelecer o padrão de atendimento aplicável aos dados pessoais coletados dentro das fronteiras. Os exemplos incluem o regulamento geral de proteção de dados da UE (GDPR), a lei de proteção de dados pessoais da Índia e a lei de proteção de dados pessoais da Tailândia.

Embora as especificidades dessas leis variem, as preocupações por trás delas são universais. Uma é a crença, verdadeira ou não, de que os dados são mais seguros em seu próprio país, protegidos pelas leis de seu país. Outra é a preocupação de que a aplicação da lei, seja estrangeira ou nacional, possa obrigar um provedor de serviços a entregar dados do cliente sem o conhecimento ou o envolvimento do cliente. As empresas que usam serviços em nuvem precisam avaliar esses riscos em relação aos benefícios da nuvem: adoção rápida, escalabilidade e inovação contínua.

Formas de limitar a exposição de dados de clientes

Aplique os controles técnicos. Minimize os dados coletados e mantenha-os apenas pelo tempo que for necessário ou exigido por lei. Use criptografia avançada e controle de acesso para proteger o conteúdo do cliente.

Use controles legais. Se os governos solicitarem acesso aos dados do cliente, primeiro tente redirecionar o solicitante para o cliente ou o proprietário dos dados. Recorra ao processo legal disponível para contestar solicitações que invadem injustificadamente a privacidade ou outros direitos do cliente.

Seja estratégico quanto aos locais dos data centers. Considere como a localização de data centers em diferentes partes do mundo afetará os clientes. Se eficientes, os controles de administração de dados podem melhorar a experiência geral do usuário, por exemplo, oferecendo aos clientes alguma medida de controle sobre seu conteúdo e como eles gerenciam dados. Se possível, considere permitir que os clientes escolham a região em que seus dados são armazenados para atender aos requisitos de soberania, privacidade ou latência.

O futuro dos dados: soberania digital

A mesma tecnologia que viabiliza nosso mundo interconectado via Internet também criou complexidades sobre a soberania de dados. Os países estão reagindo à digitalização de suas economias e ao vasto acervo de dados que ela cria, ao se basearem no conceito de soberania para afirmar a autoridade suprema sobre os dados e garantir o controle e a proteção dos dados. “Meus dados, minha lei” é agora a nova norma. Em todo o mundo, novas estruturas de dados apontam para barreiras nacionais à movimentação de dados, acesso a dados, uso e armazenamento de dados.

Embora bem-intencionada, essa abordagem restrita ameaça diminuir os benefícios econômicos possibilitados pela tecnologia moderna. Uma estrutura nova e inovadora deve emergir, reforçando os direitos dos proprietários de dados e a soberania nacional, mas confiando na tecnologia, e não apenas na lei, para atingir esse objetivo. A criptografia avançada, a computação confidencial, a ofuscação e outras tecnologias e técnicas emergentes de melhoria da privacidade (PETs) prometem criar um modelo de soberania digital em uma Internet segura, aberta e dinâmica.

[1]Princípios de administração de dados da economia digital global, centro de estudos estratégicos e internacionais

Seja transparente

Divulgue todas as informações necessárias para que os clientes façam escolhas fundamentadas

A transparência acontece quando fatos relevantes sobre uma empresa são disponibilizados aos clientes de forma oportuna e eficiente.

A transparência vai além do cumprimento dos regulamentos relativos a divulgações. Ela mostra como você lida com operações comerciais, conteúdo do cliente e informações de privacidade, incluindo:

- Quais dados você coleta e como você os usa e protege
- Como você respeita os direitos do titular dos dados
- Os principais detalhes de suas políticas sobre a divulgação de violações e vulnerabilidades de segurança
- Como você responde às solicitações do governo por dados
- Quais são seus planos de continuidade dos negócios

Em geral, uma empresa transparente está confiante de que seu tratamento de dados é justo, ético e responsável. Toma as medidas certas para proteger os dados do cliente e respeitar a privacidade. E está disposta a divulgar publicamente as políticas, os processos e a tecnologia que usa para proteger dados. As manchetes recentes tornaram as empresas mais conscientes dos custos financeiros e de reputação da segurança inadequada.

Maneiras de aumentar a transparência

Facilite para que os clientes encontrem as informações que procuram. Pergunte aos clientes o que eles querem saber — e então forneça sem que eles procurem. Use uma linguagem simples e clara.

Divulgue publicamente todas as vulnerabilidades importantes. Isso se aplica se a vulnerabilidade for descoberta internamente ou por terceiros. Ajude os clientes a entender e gerenciar riscos.

Notifique todas as pessoas afetadas por uma violação ao mesmo tempo. O direito à transparência se aplica igualmente a todos os clientes afetados, independentemente do tamanho ou do setor.

Defenda os clientes quando os governos solicitarem dados. Mostre que segue a lei e tentará proteger as informações do cliente contra solicitações ilegais. Quando legalmente permitido, notifique o cliente sobre a solicitação. Sempre que possível, a solicitação deve ir diretamente para o cliente, não para o provedor de serviços de TI. Quando solicitado pelo cliente, ajude-o a preservar ou produzir o conteúdo solicitado.

> *"Quando surgem problemas de segurança, é importante que os clientes entendam como eles serão abordados. Cumprir essa promessa requer um processo rigoroso para gerenciar o recebimento, a investigação e o relatório das informações de vulnerabilidade de segurança."*
>
> **Anthony Grieco**
> Vice-presidente, diretor executivo de segurança da informação, Cisco

> *"A transparência começa com a cultura. É uma expectativa de que os funcionários sejam responsáveis pela forma como interagem com os clientes e o mundo em geral."*
>
> **Noelle Warburton**
> Diretora de segurança e confiança em comunicações estratégicas, Cisco

Prove.

Demonstre a conformidade com a verificação independente por terceiros

Os outros pilares do New Trust Standard são os compromissos essenciais, com a transparência, uma abordagem de zero trust para acesso à rede, soberania de dados e uma cadeia de fornecimento confiável. As certificações são a prova de que a empresa mantém esses compromissos. As certificações de segurança de produtos comuns incluem o padrão internacional ISO/IEC 27001, System and Organization Controls (SOC 2) na América do Norte, FedRAMP no setor público dos EUA e Cloud Computing Compliance Controls Catalog (C5) na Alemanha.

Para obter certificações, os provedores de produtos e serviços de TI passam por uma auditoria por um terceiro independente e credenciado, geralmente uma empresa de contabilidade. Nos EUA, por exemplo, os auditores recebem acreditação do Conselho Nacional de Acreditação (ANAB) da ANSI-ASQ. As certificações de privacidade demonstram para clientes, reguladores e outras partes interessadas que o fornecedor defende os princípios de privacidade reconhecidos internacionalmente e respeita os direitos fundamentais dos titulares dos dados ao lidar com as PII. As certificações reconhecidas incluem regras corporativas vinculativas da UE, regras de privacidade transfronteiriça da APEC, reconhecimento de privacidade da APEC para processadores e o Privacy Shield EUA (inválido para transferências da UE, mas ainda reconhecido pelos EUA). Essas certificações são administradas e verificadas por reguladores de privacidade ou agentes de responsabilidade independentes aprovados pelo regulador.

As certificações se tornam cada vez mais importantes em um mundo na nuvem

Quando você compra hardware ou software para implantar em seu próprio data center, os dados da empresa ou do cliente nunca saem do seu prédio. Você só precisa confiar que o produto fará o trabalho. Quando você assina um serviço em nuvem, por outro lado, os dados do cliente e da empresa saem de suas instalações. Eles residem nos servidores do provedor e viaja pela rede do provedor. Agora você também precisa confiar que o provedor de serviços lida com os dados do cliente de forma responsável. Faz correções e atualizações em tempo hábil. Está em conformidade com os requisitos de soberania de dados. Gerencia vulnerabilidades. Atende a contratos de nível de serviço para disponibilidade. Respeita os direitos de privacidade dos titulares de dados. A evolução constante dos serviços em nuvem também inclui a evolução dos controles de segurança. As certificações anuais fornecem uma medida confiável do perfil de segurança de um fornecedor e oferecem aos clientes uma maneira mais fácil de fazer escolhas informadas.

"As certificações de privacidade são importantes. Noventa por cento das empresas entrevistadas indicaram que as certificações de privacidade ISO, APEC e UE são fatores importantes que afetam a seleção do fornecedor e as decisões de compra."

Harvey Jang
Vice-Presidente, diretor de privacidade, Cisco

Fonte: Estudo comparativo de privacidade de dados - Cisco 2021

Conclusão

O New Trust Standard diz que a confiança não se resume mais à intuição. Não é mais uma declaração inspiracional na página dos valores corporativos. Tendo visto os riscos quando dados confidenciais entram em mãos erradas, os clientes de hoje são mais exigentes. Eles querem garantia tangível de que as empresas com as quais trabalham têm comprometimento, tecnologia e processos para proteger seus dados. A capacidade de as empresas enfrentarem o desafio afetará não apenas seus resultados, mas também a continuidade da infraestrutura essencial da qual a sociedade depende.

Na Cisco, o New Trust Standard mudou a forma como fazemos negócios. Estamos ouvindo o que nossos clientes querem, implantando a tecnologia, os processos, as políticas e as pessoas para oferecer, e trabalhando ao lado deles para mapear um futuro digital com confiança na base.

Algumas de nossas ações: criamos uma arquitetura zero trust. Redigimos nossos contratos com fornecedores para responsabilizá-los pelos mesmos padrões de segurança e privacidade que nos comprometemos a manter. Publicamos e seguimos uma Abordagem baseada em princípios para solicitações de dados do governo. Publicamos os Data sheets de dados de privacidade de produtos e serviços que processam dados pessoais, respondendo a perguntas comuns dos clientes em detalhes suficientes para que eles possam decidir a melhor e mais segura maneira de usar o produto para atender às suas necessidades. E obtemos certificações de segurança e privacidade para que os clientes não precisem basear sua confiança em nossos produtos apenas na fé.

Iniciado pelos clientes, o New Trust Standard é um desenvolvimento positivo para nosso mundo cada vez mais digital. Declarar explicitamente o que os clientes esperam das empresas com as quais fazem negócios transforma a confiança em um sentimento para um referencial objetivo.

Para saber mais sobre o compromisso da Cisco com a confiança, acesse trust.cisco.com.

© 2021 Cisco e/ou suas afiliadas. Todos os direitos reservados. Cisco e o logotipo da Cisco são marcas comerciais ou marcas comerciais registradas da Cisco e/ou de suas afiliadas nos EUA e em outros países. Para obter uma lista das marcas comerciais da Cisco, acesse: www.cisco.com/go/trademarks. Todas as marcas de terceiros citadas pertencem a seus respectivos detentores. O uso do termo "parceiro" não implica uma relação de sociedade entre a Cisco e qualquer outra empresa.