Verifique tudo. Não confie em nada.

Ambientes virtuais levam governos a um modelo de segurança de confiança zero

Fevereiro de 2022

Um dos executivos da sua empresa está voltando de uma reunião para casa. Ele sai do metrô para pegar o próximo trem e percebe que não está com o seu celular, que armazena uma quantidade enorme de dados confidenciais e acesso ao sistema de sua empresa. Ele entra em pânico ao ver o trem se afastar da plataforma. Qual é o tamanho desse risco para a empresa e para os cidadãos?

A segurança cibernética em um mundo virtual é drasticamente diferente do que a defesa de sistemas e informações dentro de um ambiente físico definido. Os usuários estão por toda parte. Os dados se espalham por todos os lugares. Um modelo de segurança de confiança zero (*Zero Trust*) pode minimizar as ameaças nos ambientes digitais virtuais.

Situação atual

As abordagens tradicionais de segurança cibernética com controles limítrofes eram adequadas quando os dados ficavam hospedados e as pessoas trabalhavam em locais específicos. Sem os limites físicos, essas perspectivas não funcionam mais. Elas também criam gargalos e experiências ruins ao usuário. A segurança tradicional deve se tornar mais ágil para proteger dados, redes, informações e identidades, mantendo a agilidade que o modelo em nuvem, a mobilidade e o trabalho remoto oferecem.

Para se ter uma ideia das possibilidades do modelo de *Zero Trust*, ele poderia, por exemplo, entender se a pessoa que pegou o celular perdido não o segura como o seu proprietário. A tecnologia também reconheceria que o manuseio dessa pessoa no dispositivo é diferente. A tecnologia então transmitiria as informações para o centro de operações de segurança, onde seria possível avaliar a situação em tempo real e resolver o caso.

Conforme a tabela à direita mostra, uma estrutura de *Zero Trust*, além de oferecer segurança estática, pode proteger melhor os ativos, dados e serviços. Isso é especialmente verdadeiro considerando os desafios cibernéticos mais intensos criados atualmente pela força de trabalho virtual, os dispositivos móveis e as operações baseadas na nuvem. As organizações não podem mais confiar nas identidades dos usuários, nos seus dispositivos, nas informações, nas redes ou nos dados.

Por exemplo, com a inteligência atual do gerenciamento de identidades, as organizações podem realizar avaliações de risco mais inteligentes para qualquer recurso na nuvem. Adicionar uma autenticação multifator é um passo em direção ao *Zero Trust*.

Uma tecnologia similar pode rastrear *logins* suspeitos, ao monitorar o horário em que um usuário normalmente inicializa ou abre o sistema, e a partir de qual tipo de dispositivo. Talvez o comportamento do usuário seja normal, mas há uma tentativa de *download* de uma grande quantidade de dados, o que pode ser uma ameaça.

Estrutura de *Zero Trust*

Automação e orquestração		**Governança**
	Identidade	MFS/RBAC Gerenciamento de privilégios Privilégios menores Prova de identidade
	Dispositivo/ informações	Saúde/postura do dispositivo Detecção e resposta de terminal API/Microsserviços Código de segurança
	Rede	Roteamento dinâmico e microssegmentação NGF/*Gateway* via *web/proxy* Introspecção de tráfego Limite definido por *software*
	Dados	Classificação CASB/DLP/MDM Criptografia/ofuscação
		Visibilidade e análises

O que o *Zero Trust* pode alcançar?

Atingir a sua missão é o foco principal de toda organização. Não confiar em nada ou em ninguém pode parecer difícil, mas é o que as organizações precisam fazer. O modelo *Zero Trust* significa conhecer seus dados, onde eles estão e facilitar o acesso a eles. Isso inclui um forte gerenciamento de identidades, redes modernas e capazes definidas por *software* e análises avançadas, com o objetivo de ajudar a:

— **Melhorar a detecção de ameaças.** As organizações tomam conhecimento da ação mais cedo e têm uma cenário mais claro do ataque, seja ele interno ou proveniente de um agente malicioso externo.

— **Minimizar a perda de dados,** protegendo o acesso aos dados, não importando onde o aplicativo, sistema ou usuário esteja.

— **Reduzir o risco, melhorar a postura de segurança e ajudar a aplicar as políticas de segurança.** Aqueles que pretendem causar danos continuam se tornando mais sofisticados e usando tecnologias e táticas avançadas. As organizações devem permanecer à frente dos adversários com as proteções mais avançadas.

— **Manter a confiança.** Os cidadãos confiam nas instituições governamentais para proteger dados pessoais confidenciais. Uma vez que uma notícia sobre violação de segurança é divulgada e a organização perde a confiança do público, é difícil reconstruí-la.

— **Preparar as organizações para o que está por vir.** Conforme os ataques cibernéticos melhoram com inteligência artificial e aprendizado de máquina, um modelo de *Zero Trust* coloca as organizações à frente dos invasores que pretendem prejudicá-las.

Como o *Zero Trust* funciona?

Conforme as organizações governamentais migram para a nuvem e os funcionários continuam trabalhando remotamente, as defesas estáticas e com limites definidos não são mais adequadas. No entanto, o *Zero Trust* envolve várias ações, não apenas implementações de tecnologia. Portanto, um planejamento é fundamental. Os modelos de *Zero Trust* usam vários componentes e, de maneira similar às peças de um quebra- cabeça, cada componente deve se ajustar para criar um ambiente de segurança cibernética coeso. O planejamento de uma reestruturação incremental e sequencial aumenta o sucesso e pode ajudar a manter os recursos necessários.

Os líderes governamentais podem não perceber que suas organizações já têm a maior parte dos componentes necessários para melhorar sua defesa, como a prova de identidade ou o planejamento como parte da segurança cibernética ou da nuvem. O *Zero Trust* também torna necessário educar os funcionários para ajudar a construir uma cultura cibernética.

Como as ameaças cibernéticas podem ter origem em qualquer lugar, não é possível confiar na identidade do usuário, no dispositivo ou nas informações fornecidas, na rede ou nos dados.

Um forte sistema de gerenciamento de identidades cria, armazena e gerencia contas de usuários e registros de **identidade**. É necessário haver políticas fortes de provisionamento e autenticação de usuários antes de mudar para uma implementação alinhada com o modelo *Zero Trust*. O acesso a esses recursos deve incluir o sistema solicitante, a identidade do usuário e as características comportamentais observáveis. Como a autenticação do usuário é um ciclo constante de acesso, varredura, avaliação, adaptação e autenticação, a arquitetura de *Zero Trust* deve ser projetada para que cada usuário receba apenas os recursos mínimos do sistema para realizar a sua função.

Definição de *Zero Trust*

Zero Trust é uma perspectiva de segurança cibernética e gerenciamento de risco que protege o ambiente, não importando onde os dados e as pessoas estejam. Não é um produto. É uma estrutura ou modelo que as áreas de TI e as organizações usam para desenvolver a capacidade de não confiar em nada e verificar tudo.

O *Zero Trust* também depende de um inventário preciso e detalhado dos dispositivos dos funcionários. Os equipamentos precisam ser protegidos com um recurso de detecção e resposta de terminal, que monitore os dispositivos e reduza as ameaças cibernéticas continuamente. Toda a cadeia de suprimentos, incluindo empresas, produtos e serviços, também precisa ser protegida.

Com o modelo de *Zero Trust*, os *firewalls* centrados na rede não são mais eficazes. Em vez disso, é necessário redefinir o acesso aos aplicativos com um serviço perimetral definido por *software* (*software-defined perimeter*, em inglês — SDP). Isso inclui microvirtualização (isolamento no nível dos aplicativos do sistema operacional) e microssegmentação (divisão da rede e redução do número de usuários por segmento de rede) no SDP. Essa estratégia também mantém a visibilidade cibernética em contêineres e o tráfego criptografado.

O objetivo do *Zero Trust* é proteger os dados. A segurança de dados abrange uma ampla gama de tecnologias e *softwares*, incluindo sistemas de prevenção de perda de dados, criptografia, monitoramento da integridade de arquivos e limpeza de dados. Os dados precisam ser criptografados em repouso, em movimento e até mesmo durante o processamento. As análises criptografadas são possíveis usando criptografia homomórfica. O *software* de controle de segurança de acesso à nuvem fica hospedado entre usuários e aplicativos na nuvem, monitora a atividade e aplica políticas de segurança para proteger os dados armazenados na nuvem.

Para demonstrar conformidade, as organizações devem considerar o valor dos dados em todo o ciclo de vida de dados. A segurança deles deve oferecer apoio a várias estruturas de informações e tipos de ativos para enfrentar as ameaças e preocupações específicas e integrar controles com ambientes locais e em nuvem.

Situação atual

O maior desafio para as áreas de TI e de segurança da informação é comunicar a extrema necessidade do *Zero Trust* para proteger a organização. Os líderes e equipes de segurança cibernética devem ser capazes de articular a necessidade da mudança antes de iniciar a jornada, que inclui a solicitação de recursos. Aqui estão algumas etapas a serem seguidas que justificam a implementação do modelo de *Zero Trust:*

— **Formar uma pequena equipe central** de segurança e das áreas do negócio e desenvolver o planejamento do modelo de *Zero Trust*.

— **Avaliar** o ambiente de segurança cibernética com base na arquitetura que a organização precisa e concluir uma análise dos *gaps* para identificar os pontos fracos.

— **Criar um roteiro personalizado** para alcançar a situação desejada de segurança, risco e *compliance*.

— **Desenvolver políticas** processos e diretrizes para o novo ambiente.

— **Selecionar a tecnologia** e os serviços necessários.

— **Implementar** as ações de forma contínua de acordo com o seu plano.

— **Incluir o gerenciamento de mudanças organizacionais** em todo o processo para uma implementação bem-sucedida, uma vez que alguns componentes necessários para um modelo de *Zero Trust* exigem mudanças de funções e processos de trabalho.

A KPMG ajuda as organizações a implementar modelos de *Zero Trust*, começando com avaliações e ajudando a criar roteiros durante toda a implementação. Com a experiência e conhecimento em sistemas e processos de instituições governamentais e seus desafios cibernéticos complexos, além de suas operações e culturas, é possível determinar o melhor método e as opções de tecnologia para solucionar os desafios de segurança cibernética mais complexos e urgentes. Ao mesmo tempo, é possível fortalecer a capacidade de enfrentamento das ameaças emergentes e em evolução.

Regulamentações de segurança cibernética, agentes mal-intencionados, desastres naturais e acidentes não diminuirão enquanto os líderes da organização refletem sobre suas próximas etapas em segurança cibernética. O planejamento ou continuação da implementação do modelo de *Zero Trust* o mais breve possível contribuirá para as organizações estejam mais preparadas para imprevistos futuros.

Rastrear atividades suspeitas

Imagine um servidor, aplicativo ou um membro da equipe — cada um deles já autenticado — tentando entrar em um sistema para o qual não tem autorização de acesso. É assim que os invasores podem obter o controle de um ambiente e como as violações de *malware* ou de dados ocorrem. Em um modelo de *Zero Trust*, a tecnologia detecta atividades suspeitas e impede a comunicação com aplicativos, servidores, locais ou contas não autorizados.

Fale com o nosso time

Leandro Augusto
Sócio-líder de Cyber Security
da KPMG no Brasil
lantonio@kpmg.com.br

Tony Hubbard
Sócio-líder de Cyber Security
Governamental da KPMG nos
EUA
thubbard@kpmg.com

Joseph Klimavicz
Sócio-diretor de Advisory e de
TI da KPMG nos EUA
jklimavicz@kpmg.com

Kathy Cruz
Sócia-diretora de Tecnologia
Governamental e Treinamento
da KPMG nos EUA
kathycruz@kpmg.com

Ser digital
transforma negócios.

#KPMGTransforma

Baixe o
nosso APP

kpmg.com.br
/kpmgbrasil