O QUE É UMA ARQUITETURA ZERO TRUST?

As empresas que desejam impedir de forma confiável a exfiltração de dados confidenciais e melhorar sua capacidade de defesa contra as ameaças virtuais modernas, devem considerar uma arquitetura *Zero Trust*. Introduzido pela empresa de análise Forrester Research, o *Zero Trust* é uma arquitetura alternativa para a segurança de TI, baseada no princípio de "nunca confiar, sempre verificar".

Os modelos de segurança convencionais atuam com base na suposição de que tudo que, está no interior da rede de uma organização pode ser confiável, mas, devido à crescente sofisticação de ataques e ameaças internas, novas medidas de segurança precisam ser tomadas para impedir grandes desastres e prejuízos. E como os modelos tradicionais de segurança são projetados para proteger o perímetro, as ameaças que ficam dentro da rede são deixadas invisíveis, não inspecionadas e livres para se transformar e mover-se onde quer que desejem para extrair com êxito dados comerciais importantes e valiosos.

A arquitetura *Zero Trust*, baseada neste princípio de "nunca confiar, sempre verificar", é projetada para tratar do movimento de ameaças laterais dentro da rede, aproveitando a aplicação da micros-segmentação e dos perímetros granulares, com base no usuário, nos dados e na localização. O movimento lateral define diferentes técnicas que os atacantes usam para percorrer uma rede em busca de ativos e dados valiosos.

“Lembre-se, o ponto de infiltração de um ataque geralmente não é o local de destino, e assim a razão que impede o movimento lateral é tão importante.”

Por exemplo, se um invasor se infiltra em um endpoint, talvez ele ainda precise mover-se lateralmente pelo ambiente para acessar o data center em que reside o conteúdo segmentado ou, se o phishing da credencial for usado com êxito, essas credenciais devem ser autenticadas no banco de dados para alcançar o localização dos dados que um invasor está tentando extrair.

Como você define o movimento ou o acesso é baseado em quem é o usuário e na interação apropriada definida. Por exemplo, na maioria das organizações, os usuários em marketing poderiam acessar bancos de dados com conteúdo de marketing, conteúdo do cliente e Salesforce, mas não teriam acesso a arquivos ou dados financeiros; os usuários em finanças podem ter acesso a bancos de dados relacionados a finanças, mas não informações de RH; e assim por diante.

É fundamental identificar quem são os usuários, quais aplicativos eles estão tentando alcançar e se a ação é considerada uma sessão apropriada. Se essas junções ou pontos de inspeção não estiverem no lugar, você não poderá identificar o tráfego para interromper o movimento.

Basicamente, o Zero Trust é uma forma de mudar o que você pensa sobre segurança:

- **Garanta que todos os dados e recursos sejam acessados com segurança, com base no usuário e no local.** Você deve identificar o tráfego e o fluxo de dados que mapeia para seus fluxos de negócios e, em seguida, ter visibilidade para o aplicativo, o usuário e os fluxos. Entender quem são os usuários, quais aplicativos eles estão usando e o método de conexão apropriado é a única maneira de determinar e reforçar a política que garante acesso seguro aos seus dados.

- **Adote uma estratégia de acesso menos privilegiada e aplique rigorosamente o controle de acesso.** Ao fazer isso, as empresas podem reduzir significativamente os caminhos para invasores e malwares.

- **"Sempre verifique", o que significa inspecionar e registrar todo o tráfego.** Para fazer isso de forma eficaz, identifique as junções apropriadas para inspeção e construa os pontos de inspeção. As regras de segurança, baseadas nas políticas de negócios, devem ser usadas para identificar e permitir ou negar que o tráfego e a atividade percorram os “pontos de inspeção” que controlam, barrando em seus sub-perímetros. Isso permite a segmentação de recursos confidenciais e estabelece limites de confiança para ajudar a evitar a exfiltração de dados confidenciais.

- **Adicione mais métodos de autenticação para combater ataques baseados em credenciais.**

- **Nunca confie, sempre continue adicionando contexto e mantenha suas funções atualizadas.**

Como conseguir uma arquitetura de confiança zero?

Use o Zero Trust para obter visibilidade e contexto para todo o tráfego - entre usuário, dispositivo, local e aplicativo - além de recursos de zoneamento para visibilidade do tráfego interno. Para ganhar visibilidade e contexto do tráfego, ele precisa passar por um firewall de próxima geração (NGFW) com recursos de descriptografia. O firewall de próxima geração permite a micros-segmentação de perímetros e atua como controle de fronteiras dentro de sua organização.

Embora seja necessário proteger a borda do perímetro externo, é ainda mais crucial obter visibilidade para verificar o tráfego, na medida em que ele passa entre as diferentes funções da rede. Adicionar dois fatores de autenticação e outros métodos de verificação aumentará sua capacidade de verificar os usuários corretamente. Utilize uma abordagem de confiança zero para identificar seus processos de negócios, usuários, dados, fluxos de dados e riscos associados.

Para saber mais sobre confiança zero no data center, assista o webinar “Como habilitar a segurança de confiança zero para seu data center” ou leia o whitepaper “Como começar com uma abordagem de confiança zero para segurança de rede” . Há também o whitepaper “Cinco etapas para uma rede de confiança zero” , da Forrester Research, para ajudar na implementação nas empresas prontas para dar o próximo passo.

Ainda tem dúvidas? Chame-nos no WhatsApp!

ou envie seu e-mail para comercial@gantech.com.br

www.gantech.com.br