Zero Trust: um conceito de segurança para o mundo digital

ÍNDICE

O que é confiança zero ou Zero Trust?

Como funciona o Zero Trust?

Pilar I: sempre verifique usuários e dispositivos



O que é confiança zero ou Zero Trust?

“Não confie em ninguém” – Este lema pode soar familiar para os fãs de Arquivo X que seguiram os agentes do FBI Mulder e Scully em suas aventuras paranormais em meados da década de 1990. A segurança cibernética reflete exatamente esse lema: não confie em ninguém dentro e fora de sua

organização por padrão, mesmo que um usuário, dispositivo ou aplicativo opere dentro da rede de confiança da empresa. Zero Trust é uma estratégia de segurança que reage aos novos desafios que surgem com a digitalização, que é especialmente importante para as empresas.

Quando pensamos alguns anos atrás, a noção mais comum era que as redes internas da empresa são sempre seguras e que todas as conexões, dispositivos, usuários e softwares provenientes dessa rede interna podem ser automaticamente confiáveis. Se um hacker tentasse atacar, provavelmente seria de uma fonte externa. O foco estava na segurança do perímetro, onde você isola sua rede do mundo exterior e luta contra intrusos nos portões.

No entanto, essas velhas formas de pensar sobre segurança de rede estão desatualizadas e a segurança de perímetro por si só está se tornando cada vez mais ineficaz contra as ameaças cibernéticas atuais. O que funcionou na década de 1990, quando as estruturas de rede eram mais simples e os dispositivos menos conectados, não se harmoniza mais com o complexo mundo online de hoje. Hoje, tudo está interconectado, os serviços em nuvem estão crescendo e o trabalho remoto se popularizou, deixando as redes das empresas mais vulneráveis do que nunca e ofuscando a definição do que podemos definir como perímetro.

Além disso, o passado mostrou que as ameaças cibernéticas podem definitivamente vir de dentro de uma rede corporativa selada. Isso pode ser deliberado (no caso de um funcionário ser desonesto) ou não intencional (malware instalado acidentalmente ou golpistas que parecem muito confiáveis). Os funcionários geralmente são o elo mais fraco, portanto, as medidas de segurança precisam estar o mais próximo possível das pessoas. É aí que entra a estratégia Zero Trust, que oferece às empresas diretrizes de segurança que visam prevenir ciberataques e minimizar a vulnerabilidade das redes das empresas.

Como funciona o Zero Trust?

Zero Trust é uma estratégia de segurança centrada no usuário. Em essência, isso implica que nem o usuário nem o dispositivo podem ser confiáveis, desde o CEO até o representante de atendimento ao cliente. O conceito é baseado principalmente em 3 pilares principais e busca confirmar repetidamente a identidade de um funcionário para todas as transações importantes e solicitações de acesso. Restringir o acesso a dados confidenciais e sempre assumir que uma violação de segurança pode ocorrer a qualquer momento também está incluída no Zero Trust.

Vamos dar uma olhada em cada pilar para obter mais detalhes sobre como esse conceito de segurança pode parecer em um ambiente de negócios diário:

Pilar I: sempre verifique usuários e dispositivos

Qual funcionário está fazendo login na conexão VPN da empresa e de, qual dispositivo? Os usuários são realmente quem eles dizem que são apenas porque estão usando um crachá da empresa? A Zero Trust contesta esse fato (“nunca confie, sempre verifique”), considerando bastante ingênuo pensar que uma credencial ou endereço de e-mail e senha são formas únicas e seguras de provar a identidade de alguém.

Dispositivos e crachás podem ser roubados, credenciais podem ser hackeadas. A aplicação de autenticação multicamada para reconfirmar a identidade dos funcionários e seus dispositivos a