PHISHX

Confiança Zero

Confiança Zero

A maioria dos sistemas atualmente são construídos considerando que alguém que possua login e senha, é confiável. A segurança existe para impedir que quem não tenha a senha entre. Porém, quando ambientes remotos começam a se tornar mais comuns, nós não temos mais como saber se dá para confiar em todo mundo.

Confiança Zero é uma forma de pensar a segurança da sua organização. Considerando que a maior parte dos ataques cibernéticos envolvem credenciais, isso significa que existem riscos e vulnerabilidades dentro dos métodos utilizados atualmente.

Assim, esse modelo de segurança surge para controlar os recursos corporativos, definindo quais dados, aplicativos, dispositivos e serviços devem ser protegidos.

Como aplicar a Confiança Zero

A metodologia da Confiança Zero busca compreender o que já está na rede. Nem tudo que é armazenado tem a mesma importância. Dessa forma, é preciso listar o que exige mais segurança, assim é possível destinar mais recursos para garantir que dados e sistemas sensíveis estejam protegidos.

A partir do momento que temos a lista daquilo que precisa de segurança máxima, entre dados, aplicativos, dispositivos e serviços, é necessário definir as condições para acesso. O login e senha nem sempre são suficientes.

Para aplicar esse modelo de segurança, é preciso seguir alguns pontos fundamentais. Primeiro, ter visibilidade sobre os ativos que serão protegidos, monitorando todos. Depois, a organização precisa implementar políticas para controlar o acesso de ativos específicos, para que somente pessoas específicas sejam autorizadas.

Por fim, a automação de processos permite que as políticas sejam disseminadas e aplicadas corretamente. Além disso, automatizar o processo também auxilia o monitoramento e a tomada de decisões.

Adotando estratégias

O trabalho remoto permitiu que as pessoas acessassem recursos corporativos de diferentes locais. Isso faz com que esses recursos não estejam totalmente protegidos. Alguns deles podem ser acessados com credenciais, como aqueles que não contenham informações importantes.

Mas, seguindo os métodos aplicados pela estratégia de Confiança Zero, aqueles recursos que são considerados essenciais devem conter outras camadas de segurança. Dessa forma, os recursos podem estar protegidos quando acessados de lugares pouco protegidos, como redes públicas.

Pode ser que o acesso seja permitido apenas para dispositivos específicos. Ou até mesmo permitindo que uma aplicação só seja acessada a partir de uma rede local do prédio da sua organização.

Existem diferentes estratégias dentro dos modelos de Confiança Zero. Controlar o tráfego de informações de dispositivos, dados, serviços ou aplicativos considerados importantes também é um dos métodos utilizados.

Limitar a quantidade de usuários que acessam esses recursos corporativos também pode ser um dos passos para aplicar esse tipo de modelo.

Por que esse modelo é mais seguro?

A Confiança Zero exige analisar os recursos de sua organização e saber as formas que eles são utilizados. Assim, é preciso refletir sobre o que é considerado sensível e o que não é.

Como grande parte dos ataques cibernéticos começam utilizando credenciais, muitos deles poderiam ser evitados utilizando modelos de Confiança Zero. Isso porque esse modelo segmenta o acesso às informações, impedindo que uma pessoa com credenciais acesse qualquer tipo de dado, até mesmo os considerados sensíveis.

Além disso, esse modelo de segurança permite que as equipes tenham controle completo sobre os recursos corporativos, identificando possíveis ameaças e até mesmo quando dados forem roubados ou manipulados.