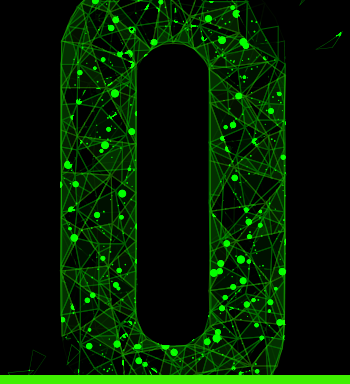

Zero Trust

O que é

Zero Trust é um conceito de segurança que parte do princípio de que ninguém e nada deve ser automaticamente considerado de confiança, mesmo dentro da rede de uma organização. Tradicionalmente, acreditava-se que as ameaças estavam apenas no exterior, mas a experiência demonstrou que ataques internos ou acessos indevidos a partir de credenciais comprometidas podem ser igualmente perigosos.

Assim, o Zero Trust baseia-se na ideia de "nunca confiar, verificar sempre". Cada tentativa de acesso a sistemas, aplicações ou dados deve ser verificada, autenticada e autorizada. Este modelo procura reduzir a probabilidade de intrusão e limitar os danos caso um ataque ocorra.

Tipos de Zero Trust

Zero Trust de Identidade
Garante que cada utilizador é autenticado de forma rigorosa, através de mecanismos como MFA ou validação contínua.

Zero Trust de Dispositivos
Verifica se o dispositivo que tenta aceder está registado, atualizado e cumpre os requisitos de segurança definidos.

Zero Trust de Redes
Divide a rede em pequenas zonas, permitindo que apenas tráfego autorizado circule em cada segmento. Desta forma, um ataque num ponto não compromete toda a rede.

Zero Trust de Dados
Protege a informação em todas as fases, quer esteja armazenada, em trânsito ou a ser utilizada. Inclui encriptação e gestão de acessos rigorosa.

Zero Trust de Infraestrutura e Cloud
Estende a proteção para ambientes híbridos e distribuídos, assegurando que a cloud obedece às mesmas regras de controlo e auditoria.

Boas Práticas

Mapear ativos críticos
Conhecer quem são os utilizadores, que dispositivos existem, quais as aplicações e onde estão os dados mais sensíveis.

Autenticação multifator (MFA)
Exigir sempre uma segunda camada de verificação para acessos importantes.

Princípio do menor privilégio
Conceder apenas as permissões necessárias a cada perfil de utilizador.

Microsegmentação da rede
Dividir a infraestrutura em zonas menores para limitar o impacto de ataques.

Monitorização contínua:
Analisar comportamentos e detetar padrões suspeitos em tempo real.

up_ motion PRR REPÚBLICA PORTUGUESA Financiado pela União Europeia NextGenerationEU