1.Ataques físicos

Os ataques cibernéticos não se limitam apenas ao ambiente digital, pois existem ameaças que exploram vulnerabilidades físicas para comprometer sistemas e redes. A segurança física desempenha um papel crucial na proteção das infraestruturas de TI, pois qualquer indivíduo que tenha acesso direto a um dispositivo pode contornar barreiras digitais e obter controle total sobre ele. Se um atacante consegue tocar fisicamente em um computador, ele pode contornar senhas, modificar configurações e até mesmo substituir componentes para obter acesso não autorizado.

Um dos métodos mais diretos de ataque físico é o uso de **força bruta**, **que não se refere apenas à quebra de senhas, mas também à tentativa de entrada forçada em um ambiente seguro**. Portas e janelas podem ser vulneráveis em data centers e salas de servidores, permitindo que invasores acessem fisicamente os equipamentos e comprometam a infraestrutura crítica. Empresas devem avaliar suas medidas de proteção física, verificando se suas instalações são resistentes a tentativas de invasão e se há controle adequado sobre quem pode entrar em áreas sensíveis.

Outro ataque físico comum é a **clonagem de RFID**, **que permite duplicar crachás e cartões de acesso utilizados para entrada em prédios e salas restritas**. A tecnologia RFID é amplamente empregada em sistemas de controle de acesso, mas sua segurança pode ser comprometida por dispositivos de clonagem baratos e facilmente encontrados online. Com um leitor RFID portátil, um criminoso pode copiar os dados de um cartão de acesso em questão de segundos e produzir uma cópia funcional. Há relatos de ataques onde criminosos conseguiram clonar cartões apenas passando próximos às vítimas em transportes públicos ou elevadores. Para mitigar esse risco, o uso de autenticação multifator é essencial, garantindo que mesmo com um cartão clonado, o invasor não consiga acessar áreas restritas sem um segundo fator de autenticação, como biometria ou um PIN.

Além dos ataques diretos a dispositivos e credenciais de acesso, os invasores podem explorar vulnerabilidades ambientais para causar interrupções nos sistemas. Um dos métodos mais simples e eficazes para comprometer um data center é desligar o fornecimento de energia, o que pode ser feito sem sequer entrar no prédio. Alguns atacantes procuram vulnerabilidades na infraestrutura elétrica e conseguem desativar o fornecimento de energia de forma remota ou manual, interrompendo a operação de servidores críticos.

Outro vetor de ataque físico envolve a manipulação dos **sistemas de climatização (HVAC)**, **que geralmente não recebem o mesmo nível de proteção que os sistemas de TI tradicionais**. Se um invasor conseguir acesso ao controle do ar condicionado de um data center, ele pode desligar os resfriadores, fazendo com que os servidores superaqueçam e se desliguem automaticamente para evitar danos. Em alguns casos, o disparo indevido de sistemas de supressão de incêndio pode causar

paralisações inesperadas, pois muitos desses sistemas são configurados para desligar a energia ao detectarem um suposto incêndio.

Diante dessas ameaças físicas, as organizações devem adotar uma abordagem de segurança que integre tanto a proteção digital quanto medidas rigorosas de controle de acesso e monitoramento ambiental. Medidas como o uso de câmeras de vigilância, portas reforçadas, autenticação multifator e monitoramento de sistemas críticos podem ajudar a reduzir os riscos e garantir a integridade da infraestrutura de TI.