1.Códigos maliciosos

Ataques cibernéticos podem ocorrer de diversas formas, desde métodos mais simples, como a exploração de credenciais padrão, até técnicas mais avançadas, como a inserção de código malicioso em sistemas. Hackers frequentemente utilizam engenharia social para enganar usuários e obter informações sensíveis, como nomes de usuário e senhas. Outra abordagem comum envolve o uso de credenciais padrão que não foram alteradas em equipamentos recém-instalados, permitindo acesso não autorizado. Além disso, erros de configuração podem deixar brechas que facilitam a invasão de redes e sistemas.

Quando essas estratégias não são suficientes, invasores recorrem a códigos maliciosos para comprometer sistemas. Esse tipo de ataque pode ser realizado por meio de arquivos executáveis, scripts, vírus de macro e cavalos de Tróia. Devido à grande variedade de métodos utilizados, é essencial adotar uma defesa robusta contra ameaças digitais. Soluções como softwares antimalware ajudam a bloquear arquivos e scripts maliciosos, enquanto firewalls impedem o tráfego de dados suspeitos. A manutenção de sistemas atualizados e a aplicação de patches de segurança reduzem vulnerabilidades exploráveis. Além disso, o treinamento de usuários é fundamental para evitar ataques de phishing e o compartilhamento involuntário de informações sensíveis.

Casos reais demonstram a gravidade dos ataques cibernéticos e a necessidade de medidas preventivas. O ransomware **WannaCry** explorou uma falha no protocolo SMB v1 do Windows, permitindo que hackers executassem código arbitrário para sequestrar sistemas e exigir pagamento pelo resgate. No ataque à **British Airways**, invasores injetaram código JavaScript malicioso nas páginas de checkout do site da empresa, capturando dados de pagamento de clientes e comprometendo cerca de 380.000 transações antes de serem detectados. Já a invasão ao **Banco de Dados de Saúde da Estônia** foi realizada por meio de injeção de SQL, permitindo que criminosos acessassem registros médicos de toda a população do país.

A diversidade de técnicas de ataque torna essencial uma abordagem proativa em segurança digital. Manter sistemas atualizados, utilizar soluções de proteção como antimalware e firewalls e promover a conscientização sobre boas práticas são medidas fundamentais para reduzir os riscos de invasões e garantir a integridade das informações.