OS DIFERENTES TIPOS DE ATAQUES CIBERNETICOS

* CONCEITOS

1. **Ransomware:** é um ataque cibernéticos no qual bloqueiam o acesso aos dados ou sistemas, exigindo pagamento de um “resgate” para restaurar o acesso. Geralmente, os dados são criptografados e ficam inacessíveis até que seja feito um tipo de pagamento. Esses ataques podem paralisar operações de negócios e resultar na perda de dados críticos, alem de expor a empresa a danos a reputação.
2. **Phishing:** É um ataque de engenharia social no qual os criminosos enviam mensagens falsas aos usuários, frequentemente por email. Assim, enganam o destinatário, fazendo com que revele informações pessoais como senhas e informações bancarias. Os emails de phishing podem parecer inofensivos, levando aos usuários a clicarem em links maliciosos ou baixar arquivos infetados.
3. **Whale-Phishing:** é uma variante sofisticada, que tem como alvo executivos e indivíduos de alto escalão em uma organização. Por envolver pessoas com acesso a dados privilegiados, o whale-phishing é ainda mais perigoso. Afinal, pode expor informações confidenciais e garantir o acesso não autorizado a determinados sistemas e recursos do negócio.
4. **DoS e DDos:** Ataques de Negação de Serviço (DoS) e Negação Distribuída de Serviço (DDos) tem como objetivo sobrecarregar sistemas, redes ou servidores com tráfego excessivo, tornando os inacessíveis para os usuários legítimos. Neste caso os criminosos virtuais podem usar uma rede de dispositivos comprometidos (Botnets).
5. **Engenharia Social:** envolve a manipulação psicológica das pessoas para que divulguem informações confidenciais ou executem ações que beneficiem o invasor. Isso pode acontecer por meio de telefonemas, mensagens falsas ou interações nas Mídias sociais
6. **Ataques de senhas:** tem como objetivo adivinhar ou roubar senha dos usuários. Em muitos casos os criminosos utilizam softwares para gerar combinações de senhas para automatizar o ataque.
7. **Falsificação de DNS:** tem como objetivo redirecionar os usuários a sites maliciosos que parecem legítimos. E com os criminosos roubam informações confidenciais como senhas de bancos e outros.
8. **Malware:** é um software malicioso projetado para infiltrar, danificar, ou controlar sistemas e dispositivos.
9. **Cavalo de troia:** é um Malware disfarçado como um software legitimo. Uma vez instalado, ele abre uma porta de entrada para os invasores, permitindo acesso não autorizado ao sistema ou rede.
10. **Spoofing:** envolve a falsificação de identidade. Ou seja, os invasores mascaram sua verdadeira identidade e fingem ser uma pessoa ou entidade confiável. É muito comum a utilização de emails, chamadas telefónicas ou sites falsos para dissimular o ataque e enganar as vítimas.