Dicionário de Segurança

- **AMEAÇA** – Possível violação de segurança de um sistema.
- **POLÍTICA DE SEGURANÇA** – Conjunto de regras que gerencia e protegem suas informações e recursos.
- **CRIPTOGRAFIA** – Política de segurança na qual somente pessoas autorizadas entenderão o significado de determinada mensagem.
- **SSL** – "S" do HTTPS, significa camada de soquete segura.
- **CRIPTOGRAFIA ASSIMÉTRICA** – Possui duas chaves , sendo uma Pública - utilizada para codificar a mensagem - e a outra, chamada de chave Privada ,utilizada para decodificar a mesma.
- **CRIPTOGRAFIA SIMÉTRICA** – Possui apenas uma chave sendo ela utilizada para codificar e decodificar a mensagem. (Privada)
- **AC** (Autoridade de Certificação) é uma entidade responsável pelo estabelecimento e a garantia de autenticidade de chaves públicas pertencentes a usuários ou a outras autoridades de certificação.
- **ASSINATURA DIGITAL** – Serve para vincular a mensagem ao usuário.
- **CONFIDENCIALIDADE** – Garantia que as informações Informações sejam privados.
- **INTEGRIDADE** – Garantia que as informações não foram alterados.
- **DISPONIBILIDADE** – Garantia que as informações estarão disponível quando necessário.
- **LEGITIMIDADE** – Garantia que origem e destino são verdadeiros.
- **AUTENTICIDADE** – Garantia que as informações são verdadeiras.
- **PRIVACIDADE** – Controle das informações acessadas, ou seja, quem acessa e sobre quais condições.
- **FIREWALL** – Sistema de proteção contra a entrada de vírus e usuários não autorizados. Política de segurança contra o Trojan (Cavalo de Tróia). Bloqueio.
- **BACKUP** – Cópia de segurança. Tipos: Normal (altera o atributo), Incremental (altera o atributo), Diferencial, Cópia e Diário.
- **TROJAN** – Um cavalo de Troia (em inglês Trojan horse) é um malware (programa malicioso) que age tal como na história do Cavalo de Troia, entrando no computador e criando uma porta para uma possível invasão.
- **SNNIFER** – Programa utilizado para invasão e controle de redes.
- **MALWARE** – Qualquer função ou programa que pode causar prejuízo.
- **VÍRUS** – Programa malicioso que necessita ser executado a fim de "agir" e causar problemas. Ele é um programa hospedeiro.
- **WORMS** – Programa malicioso que não necessita de arquivo anexo para causar problemas, sendo sua função :espalhar-se, pois possui capacidade de autorreplicação.

- **ADWARE** – Vírus de propaganda. É quando o usuário acessa um determinado site e várias janelas “pipocam” na tela sem parar.
- **SPYWARE** – Programas espiões.
- **PHISHING** – “Pescador” de informações particulares.
- **PHARMING** – Coleta de dados do usuário onde ele é jogado para uma página falsa, sendo o DNS corrompido.
- **ROOTKIT** – É um tipo de vírus que se faz presente durante a inicialização da máquina.
- **SPAM** – E-mail indesejado.
- **IDS** – Sistema de detecção de intrusos.
- **IPS** – Sistema de prevenção de intrusão; é uma forma ativa.
- **HONEY POT** – É uma invasão. Sistemas simuladores de servidores que se destinam a enganar um invasor, deixando – o pensar que está invadindo uma rede.
- **DMZ** – Nome de uma topologia de rede situada entre uma rede protegida e uma externa considerada um ótimo esquema de segurança.
- **ENGENHARIA SOCIAL** – Meio de obtenção de informações através de relações humanas de confiança ou outros métodos que enganem usuários e administradores de rede.
- **ENGENHARIA REVERSA** – Reversão de códigos já compilados para uma forma que seja legível pelo ser humano. É ilegal em alguns países.
- **BACKDOOR** – Invasão da rede através de uma porta.