SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

É A PROTEÇÃO DE SISTEMAS DE COMPUTADOR CONTRA ROUBO OU DANOS AO HARDWARE, SOFTWARE OU DADOS ELETRÔNICOS, BEM COMO A INTERRUPÇÃO OU DESORIENTAÇÃO DOS SERVIÇOS QUE FORNECEM.

https://www.youtube.com/watch?v=flu6JPRHW04&t=1s

Profª Ms. Rosiene Cazale

O AUMENTO DO ACESSO À INTERNET E A GRANDE DEMANDA POR NOVAS TECNOLOGIAS ESTÁ ACELERANDO A TRANSFORMAÇÃO DIGITAL, SEJA PELO TRABALHO REMOTO EM HOME OFFICE, APLICAÇÕES DE IOT, INTELIGÊNCIA ARTIFICIAL OU A MIGRAÇÃO DOS SERVIÇOS PARA A NUVEM, O QUE AUMENTOU A VULNERABILIDADE ATRAVÉS DE ATAQUES CIBERNÉTICOS AOS DADOS E A PRIVACIDADE.

https://www.youtube.com/watch?v=LmP6oHutn8M

PILARES DA SEGURANÇA DA INFORMAÇÃO

- **CONFIDENCIALIDADE**: PRIVACIDADE DOS DADOS DA EMPRESA. GARANTE QUE AS INFORMAÇÕES SENSÍVEIS E CONFIDENCIAIS SEJAM PRESERVADAS CONTRA ROUBOS E INVASÕES;

- **INTEGRIDADE**: CONSISTÊNCIA, PRECISÃO E CONFIABILIDADE DOS DADOS E DOS SISTEMAS DURANTE A REALIZAÇÃO DOS PROCESSOS. TAMBÉM SINALIZA QUE OS DADOS DEVEM SER ARMAZENADAS DA MANEIRA COMO FORAM CRIADOS, SEM INTERFERÊNCIAS;

- **DISPONIBILIDADE**: REFERE-SE AO TEMPO E À ACESSIBILIDADE AOS DOCUMENTOS E AOS ARQUIVOS DA COMPANHIA, JÁ QUE PRECISAM SER CONSULTADOS A QUALQUER MOMENTO.

Os invasores podem obter acesso a uma rede através de vulnerabilidades de software, ataques de hardware ou adivinhando o nome de usuário e a senha de alguém. Os invasores que obtêm acesso modificando o software ou explorando vulnerabilidades são chamados de agentes de ameaças.

Depois que o agente da ameaça obtém acesso à rede, quatro tipos de ameaças podem surgir.

- Roubo de informações
- Perda e manipulação de dados
- Roubo de identidade
- Interrupção do serviço

HACKERS WHITE HAT (CHAPÉU BRANCO)

- ÉTICOS QUE USAM SUAS HABILIDADES DE PROGRAMAÇÃO PARA FINS BONS, ÉTICOS E LEGAIS.
- UTILIZAM SEUS CONHECIMENTOS NA IDENTIFICAÇÃO DE VULNERABILIDADES DA REDE.
- AS VULNERABILIDADES DA SEGURANÇA SÃO INFORMADAS AOS DESENVOLVEDORES PARA QUE SEJAM CORRIGIDAS.
- SÃO PREMIADOS PELAS EMPRESAS INFORMADAS DAS VULNERABILIDADES

DATAPREV VAI CONTRATAR 'HACKERS DO BEM' PARA TESTAR APLICAÇÕES NA INTERNET, PARA PROCEDER A 12 TESTES E 12 RETESTES DE INTRUSÃO PARA 12 APLICAÇÕES DISPONIBILIZADAS NA INTERNET, QUE FICAM HOSPEDADAS NOS DATA CENTERS DA DATAPREV NO RIO DE JANEIRO, SÃO PAULO E DISTRITO FEDERAL. (29/07/22)

HACKERS GRAY HAT (CHAPÉU CINZA)

- ANTIÉTICOS, COMETEM CRIMES MAS NÃO PARA GANHO PESSOAL OU PARA CAUSAR DANO.
- COMPROMETEM AS REDES SEM PERMISSÃO, DIVULGAM PUBLICAMENTE A VULNERABILIDADE.
- MUITAS VEZES DIVULGAM A VULNERABILIDADE PARA À EMPRESA AFETADA.

HACKERS DO MAL

- SÃO CRIMINOSOS ANTIÉTICOS QUE VIOLAM A SEGURANÇA DO COMPUTADOR E DA REDE PARA O GANHO PESSOAL.
- ATAQUES EM UMA REDE PODEM SER DEVASTADORES E RESULTAR EM PERDA DE TEMPO E DINHEIRO, DEVIDO A DANOS OU ROUBO DE INFORMAÇÕES.

https://www.youtube.com/watch?v=9oas-skPVeg&t=16s

CIBERSEGURANÇA: O QUE SABER EM UM CENÁRIO DIGITAL EM CONSTANTE EVOLUÇÃO ?

- A GRANDE MAIORIA DE NOSSAS FINANÇAS É GERENCIADA VIRTUALMENTE, DE CONTAS BANCÁRIAS A CARTÕES DE CRÉDITO.

- NOSSOS ENDEREÇOS DE E-MAIL, SENHAS E NÚMEROS DE CARTÃO DE CRÉDITO ESTÃO VINCULADOS A SERVIÇOS DE STREAMING DE MÚSICA E FILMES.

- A TECNOLOGIA TORNA A VIDA MAIS CONVENIENTE, MAS HÁ PERIGOS ASSOCIADOS A TER NOSSAS INFORMAÇÕES ACESSÍVEIS A CIBERCRIMINOSOS EM TANTAS PLATAFORMAS DIFERENTES.

TIPOS DE VULNERABILIDADES

HÁ TRÊS TIPOS PRINCIPAIS DE VULNERABILIDADES OU PONTOS FRACOS:

VULNERABILIDADES TECNOLÓGICAS : FRAQUEZAS DO PROTOCOLO TCP/IP, DEFICIÊNCIAS DO SISTEMA OPERACIONAL E DEFICIÊNCIAS DO EQUIPAMENTO DE REDE.

VULNERABILIDADES DE CONFIGURAÇÃO: CONTAS DE USUÁRIO NÃO SEGURAS, CONTAS DO SISTEMA COM SENHAS FÁCEIS DE ADIVINHAR, SERVIÇOS DE INTERNET MAL CONFIGURADOS, CONFIGURAÇÕES PADRÃO NÃO SEGURAS E EQUIPAMENTOS DE REDE MAL CONFIGURADOS.

VULNERABILIDADES DA POLÍTICA DE SEGURANÇA: FALTA DE UMA POLÍTICA DE SEGURANÇA ESCRITA, POLÍTICA, FALTA DE CONTINUIDADE DE AUTENTICAÇÃO, CONTROLES DE ACESSO LÓGICOS NÃO APLICADOS, INSTALAÇÃO DE SOFTWARE E HARDWARE E ALTERAÇÕES QUE NÃO SEGUEM A POLÍTICA E UM PLANO DE RECUPERAÇÃO DE DESASTRES.

SEGURANÇA FÍSICA

AS QUATRO CLASSES DE AMEAÇAS FÍSICAS SÃO AS SEGUINTES:

- **AMEAÇAS DE HARDWARE** - ISSO INCLUI DANOS FÍSICOS A SERVIDORES, ROTEADORES, COMUTADORES, INSTALAÇÕES DE CABEAMENTO E ESTAÇÕES DE TRABALHO.

- **AMEAÇAS AMBIENTAIS** - ISSO INCLUI EXTREMOS DE TEMPERATURA (MUITO QUENTE OU MUITO FRIO) OU EXTREMOS DE UMIDADE (MUITO ÚMIDO OU MUITO SECO).

- **AMEAÇAS ELÉTRICAS** - ISSO INCLUI PICOS DE TENSÃO, TENSÃO DE ALIMENTAÇÃO INSUFICIENTE (QUEDAS DE ENERGIA), ENERGIA NÃO CONDICIONADA (RUÍDO) E PERDA TOTAL DE ENERGIA.

- **AMEAÇAS À MANUTENÇÃO** - ISSO INCLUI O USO DOS PRINCIPAIS COMPONENTES ELÉTRICOS (DESCARGA ELETROSTÁTICA), FALTA DE PEÇAS DE REPOSIÇÃO CRÍTICAS, CABEAMENTO INCORRETO E ROTULAGEM INADEQUADA.

TIPOS DE MALWARE (CÓDIGOS MALICIOSOS)

VÍRUS

programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos

CAVALO DE TROIA (*TROJAN*)

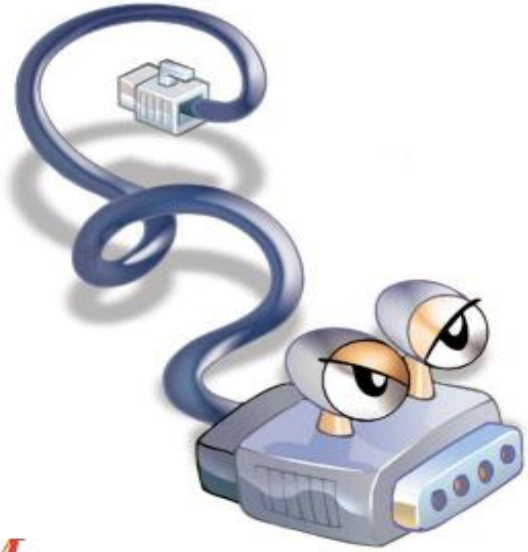
programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário

RANSOMWARE

programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário

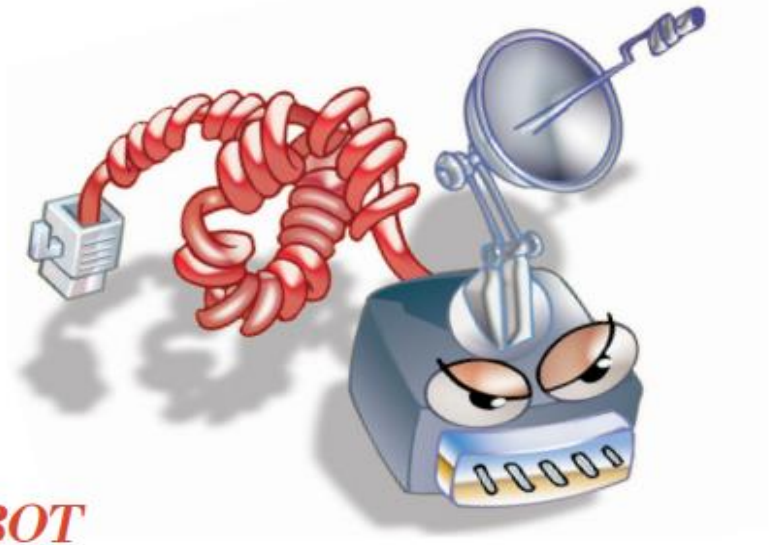
BACKDOOR

programa que permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para este fim



WORM

programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de equipamento para equipamento



BOT

programa similar ao *worm* e que possui mecanismos de comunicação com o invasor que permitem que ele seja remotamente controlado

RAT (*REMOTE ACCESS TROJAN*)

ou *trojan* de acesso remoto, é um programa que combina as características de *trojan* e de *backdoor*, já que permite ao atacante acessar o equipamento remotamente e executar ações como se fosse o usuário

ZUMBI

é como também é chamado um equipamento infectado por um *bot*, pois pode ser controlado remotamente, sem o conhecimento do seu dono

BOTNET

é uma rede formada por centenas ou milhares de equipamentos zumbis e que permite potencializar as ações danosas executadas pelos *bots*

SPYWARE

programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros

KEYLOGGER

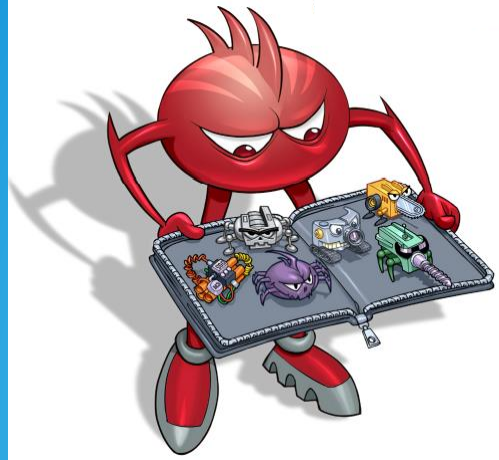
é um tipo de *spyware* capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do equipamento

SCREENLOGGER

é um tipo de *spyware*, similar ao *keylogger*, usado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking*

ADWARE

é um tipo de *spyware* projetado especificamente para apresentar propagandas



ROOTKIT

conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um equipamento comprometido

ATAQUES DE RECONHECIMENTO

OS ATAQUES À REDE PODEM SER CLASSIFICADOS EM TRÊS CATEGORIAS PRINCIPAIS:

- **ATAQUES DE RECONHECIMENTO** – DETECÇÃO E MAPEAMENTO DE SISTEMAS, SERVIÇOS OU VULNERABILIDADES
- **ATAQUES DE ACESSO** – MANIPULAÇÃO NÃO AUTORIZADA DE DADOS, DO ACESSO AO SISTEMA OU DE PRIVILÉGIOS DO USUÁRIO
- **NEGAÇÃO DE SERVIÇO** - DESATIVAÇÃO OU CORRUPÇÃO DE REDES, SISTEMAS OU SERVIÇOS.

PARA ATAQUES DE RECONHECIMENTO, EXISTEM AS FERRAMENTAS DA INTERNET, COMO AS NSLOOKUP E WHOIS, PARA DETERMINAR O ESPAÇO DE ENDEREÇO IP ATRIBUÍDO A UM HOST.

APÓS A DETERMINAÇÃO DO ESPAÇO DE ENDEREÇO IP, PODE SER EXECUTADO O COMANDO PING NOS ENDEREÇOS IP DISPONÍVEIS AO PÚBLICO PARA IDENTIFICAR OS ENDEREÇOS QUE ESTÃO ATIVOS.

ATAQUES DE ACESSO

OS ATAQUES DE ACESSO PODEM SER CLASSIFICADOS EM QUATRO TIPOS:

ATAQUES DE SENHA - IMPLEMENTADOS USANDO FORÇA BRUTA, CAVALO DE TRÓIA E FAREJADORES DE PACOTES.

EXPLORAÇÃO DE CONFIANÇA – O INVASOR USA PRIVILÉGIOS NÃO AUTORIZADOS PARA OBTER ACESSO A UM SISTEMA, POSSIVELMENTE COMPROMETENDO O ALVO.

REDIRECIONAMENTO DE PORTA: - O INVASOR USA UM SISTEMA COMPROMETIDO COMO BASE PARA ATAQUES CONTRA OUTROS ALVOS. POR EXEMPLO, USANDO SSH (PORTA 22) PARA CONECTAR-SE A UM HOST COMPROMETIDO A. O HOST A É CONFIÁVEL PELO HOST B E, PORTANTO, O INVASOR PODE USAR O TELNET (PORTA 23) PARA ACESSÁ-LO.

MAN-IN-THE-MIDDLE - O INVASOR ESTÁ POSICIONADO ENTRE DUAS ENTIDADES LEGÍTIMAS PARA LER OU MODIFICAR OS DADOS QUE PASSAM ENTRE AS DUAS PARTES.

ATAQUES DE NEGAÇÃO DE SERVIÇO (DOS)

A FORMA DE ATAQUE MAIS DIVULGADA E UMA DAS MAIS DIFÍCEIS DE ELIMINAR, MERECEM ATENÇÃO ESPECIAL DOS ADMINISTRADORES DE SEGURANÇA.

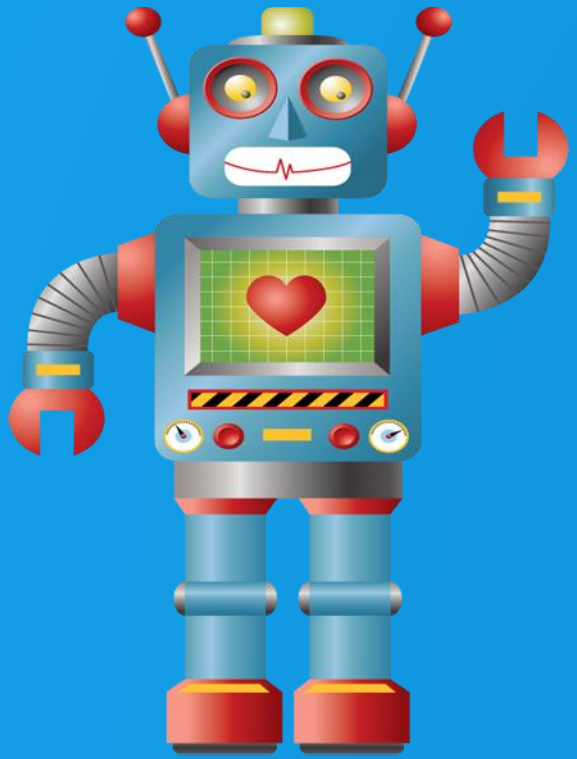
OS ATAQUES DOS ASSUMEM MUITAS FORMAS. E IMPEDEM QUE PESSOAS AUTORIZADAS USEM UM SERVIÇO AO CONSUMIR RECURSOS DO SISTEMA. PARA PREVENIR ATAQUES (DOS) É IMPORTANTE MANTER EM DIA AS MAIS RECENTES ATUALIZAÇÕES DE SEGURANÇA PARA SISTEMAS OPERACIONAIS E APLICAÇÕES.

OS ATAQUES DE DOS INTERROMPEM A COMUNICAÇÃO E CAUSAM PERDA SIGNIFICATIVA DE TEMPO E DINHEIRO. ESSES ATAQUES SÃO RELATIVAMENTE SIMPLES DE CONDUZIR, MESMO POR UM INVASOR NÃO CAPACITADO.

ATAQUES DE NEGAÇÃO DE SERVIÇO (DDOS)

UM DDOS É SEMELHANTE A UM ATAQUE DE DOS, MAS É ORIGINADO DE VÁRIAS FONTES COORDENADAS.

POR EXEMPLO, UM AGENTE DE AMEAÇA CRIA UMA REDE DE HOSTS INFECTADOS, CONHECIDOS COMO ZUMBIS. UMA REDE DE ZUMBIS É CHAMADA DE BOTNET. O ATOR AMEAÇA USA UM PROGRAMA DE COMANDO E CONTROLE (CNC) PARA INSTRUIR O BOTNET DE ZUMBIS PARA REALIZAR UM ATAQUE DDOS.



Obrigada!

Alguma dúvida?