Segurança da Informação (SI)

Princípios da SI
Atualmente, um assunto em moda cobrado pelas bancas de concursos públicos é a Segurança da Informação, tal ênfase esta diretamente relacionada com o avanço das transações pela Internet que muito favorece a um mundo globalizado.
A Internet por se tratar de uma rede pública, possui membros anônimos, que podem agir de acordo com as próprias leis, numa terra de ninguém onde questões de sigilo e privacidade se tornam primordiais, como em transações bancárias, compras com cartão de crédito e acessos remotos.
Em todos os casos, há necessidade de agir com responsabilidade, daí a necessidade de princípios para estabelecer o mínimo de segurança.

Um sistema de Segurança da Informação baseia-se em quatro princípios básicos:

D	ISPONIBILIDADE
I	NTEGRIDADE
C	ONFIDENCIALIDADE
A	UTENTICIDADE

Se um ou mais desses princípios forem desrespeitados em algum momento, significa que houve um incidente ou quebra de segurança da informação.

Disponibilidade
O princípio da Disponibilidade é garantido quando a informação está acessível, por pessoas autorizadas, sempre que necessário.
Quando um sistema está "fora do ar" por qualquer motivo ocorreu um incidente na segurança da informação por quebra da disponibilidade.
As causas de tal ocorrência podem ser as mais diversas, desde a falta de luz, incêndios, sabotagens até vírus, ataques computacionais, congestionamentos, etc.
Alguns cuidados muito comuns que versam sobre disponibilidade são: o uso de no-breaks, a manutenção dos backups e o espelhamento de discos (RAID).

Integridade
O princípio da Integridade é garantido quando a informação acessada está completa, sem alterações e portanto confiável.
Quando uma informação é indevidamente alterada, intencionalmente ou não, caracteriza um incidente na segurança da informação por quebra de integridade.
Uma técnica muito utilizada para a garantia da Integridade é o uso de funções *Hash*.

FISCAL DO CEARÁ – ESAF/2007
Nos sistemas de Segurança da Informação, existe um método que _____. Este método visa garantir a integridade da informação. Escolha a opção que preenche corretamente a lacuna acima:
a) valida a autoria da mensagem

b) verifica se uma mensagem em trânsito foi alterada
c) verifica se uma mensagem em trânsito foi lida por pessoas não autorizadas
d) cria um backup diferencial da mensagem a ser transmitida
e) passa um antivírus na mensagem a ser transmitida
Letra B!

Confidencialidade
O princípio da Confidencialidade é garantido quando apenas as pessoas explicitamente autorizadas podem ter acesso a Informação. Quando uma informação é acessada por uma pessoa não-autorizada, ocorre um incidente na segurança da informação por quebra de confidencialidade.
Técnicas como a Criptografia e a Esteganografia são utilizadas para aumentar a confidencialidade de uma informação.

Autenticidade
O princípio da Autenticidade é garantido quando se confia que a entidade que está realizando uma ação é realmente a entidade que diz ser, seja ela uma pessoa, empresa ou máquina.
Técnicas como o uso de senhas, biometria, tokens e certificados digitais podem ser utilizados para tornar autêntico o acesso às informações.

Problemas de Segurança

Vulnerabilidades
As vulnerabilidades são as fraquezas presentes nos mecanismos de comunicação que podem ser exploradas, intencionalmente ou não, resultando na quebra de um ou mais princípios de segurança da Informação.
As vulnerabilidades podem estar presentes em:

- Tecnologias
- Pessoas
- Processos
- Ambientes

Ameaça
A ameaça é um agente externo aos mecanismos de comunicação, que se aproveitando de suas vulnerabilidades poderá quebrar a confidencialidade, integridade ou disponibilidade da informação.

Ameaças Externas

Hackers e Crackers
O conceito de Hacker é o de um usuário experiente, que relacionado à informática está associado ao invasor de sistemas computacionais. Cabe destacar para as provas a diferença entre o Hacker e o Cracker: o Hacker embora aja de forma ilícita muitas vezes acabe colaborando com a segurança pois ele explora as vulnerabilidades de um sistema e as torna pública, enquanto o Cracker é o “hacker malicioso”, que vai usar seus conhecimentos para destruir sistemas, praticar fraudes ou quebrar senhas de aplicativos comerciais incentivando a “pirataria”.

POLÍCIA CIVIL – PERITO – FUNIVERSA - MARÇO/2008
No mundo cibernético, qual é o termo utilizado para designar quem pratica quebra de proteções de softwares cedidos a titulo de demonstração usando-os por tempo indeterminado como se fossem cópias legitimas.
(A) worm
(B) hacker
(C) trojan
(D) malware
(E) cracker
Letra E!

PHREAKER
É um especialista em telefonia. No passado sua principal atividade era a realização de ligações gratuitas e a instalação de escutas em telefones fixos ou celulares. Com o advento da banda larga através da telefonia móvel (3G) este cracker da telefonia tornou-se ainda mais perigoso.

Ameaças Computacionais

MALWARE (Software Malicioso)

Um Malware é um termo genérico para qualquer programa malicioso. A seguir iremos estudar os tipos de Malware.

Arquivos mais propensos a serem maliciosos (Extensões)

Alto Risco				
EXE	COM	PIF	BAT	ASP
VBS	CMD	SCR	HLP	REG

Ministério Público do RJ - Sec. de Promotoria e Curadoria – 2002
Um vírus de computador é, na verdade, um programa como outro qualquer. Ele apenas possui algumas características especiais que o assemelham a um vírus verdadeiro. Um vírus de computador NÃO pode estar armazenado:

a. em um arquivo de imagem GIF (.gif);
b. em um arquivo executável (.exe);
c. em uma página HTML (.html);
d. no servidor de arquivo de sua rede local;
e. no setor de carga (setor de boot ou boot sector) de um disco.

Arquivos de imagem, vídeo e som tem baixo risco. Letra A.

Observe que na questão anterior o examinador usou a expressão “NÃO pode”, e atualmente arquivos de imagem podem conter vírus, ainda que com pouca incidência. Logo, com relação aos vírus, devemos falar que os arquivos são mais ou menos propensos, pois na Informática, nada é impossível.

A principal porta de entrada para os malwares hoje é a Internet. Ao se baixar um arquivo ou receber um anexo por e-mail corre-se o risco de contrair um vírus de computador.
Outra maneira muito comum também é através da execução de programas contidos em unidades de memória secundária como disquetes, CD's, DVD's ou pen-drives.

TRE - Auxiliar Judiciário – 2001
Nós não podemos escolher quando vamos receber um e-mail, e muito menos que e-mail vamos receber. E para piorar, atualmente o modo mais comum de pegar vírus de computador é através de e-mail. Ao recebermos um arquivo com vírus, nosso computador fica infectado:
a) no exato momento em que o e-mail é recebido;
b)no exato momento em que o e-mail é enviado;
c) quando o nosso cliente de e-mail busca as mensagens no servidor de e-mail;
d) depois de um certo tempo após a leitura de todo e-mail, dependendo do tipo de vírus;
e)o arquivo que vem anexo contendo o vírus é aberto.
Letra E.

VÍRUS

O vírus é um programa malicioso que possui 2 objetivos básicos: Atacar e se replicar automaticamente.
Os ataques podem ser os mais variados possíveis: mensagens indevidas, erros ou lentidão na execução de programas, perda de dados, formatação indesejada do HD...
Um vírus de computador é ativado quando executamos um programa infectado.
(Agente Administrativo - Ministério da Saúde - NCE - 2005) Considere as seguintes afirmações referentes aos vírus eletrônicos:
I. Para minimizar a possibilidade de infecção por vírus é importante a instalação de um software antivírus e manter atualizado o arquivo de definição de vírus.
II. Uma mensagem de e-mail recebida a partir de um endereço confiável não pode conter vírus.
III. Um computador não conectado à Internet encontra-se livre do risco de infecção por vírus.
IV. Um vírus de computador pode tornar mais lenta a conexão da máquina infectada à Internet.
O número de afirmações corretas é:
a) 0;
b)1;
c)2;
d)3;
e)4.
I = certa, II = errada, III = errada, IV = certa, letra C.

Vírus de Arquivos
Substituem ou fixam-se a arquivos executáveis de programas, os quais sejam requisitados para a execução de algum outro programa.

Vírus de Boot

O primeiro setor físico de qualquer disco rígido de um PC contém o Registro de Partida e a Tabela de Alocação de Arquivos (FAT). Os vírus de boot visam atacar justamente essa região dos discos rígidos e disquetes. Se a FAT é corrompida, perde-se o acesso a diretórios e arquivos, não por terem sido atacados também, mas porque o seu computador não consegue mais acessá-los.

Vírus de Macro
Os vírus de macro são inimigos temidos por quem usa computadores hoje em dia. Foram descobertos em 1995 e agem de formas diferentes das citadas anteriormente. Eles infectam arquivos criados por softwares que utilizam linguagem de macro, como as planilhas eletrônicas e os processadores de texto (Microsoft Excel e Word). Os estragos variam de alterações nos comandos do aplicativo à perda total das informações.

ESCRITURÁRIO/BB/FCC/2006
Os arquivos de dados de editores de texto e de planilhas eletrônicas podem ser contaminados normalmente por programas do tipo vírus
(A) parasitas.
(B) camuflados.
(C) polimórficos.
(D) de boot.
(E) de macro.
Letra E!

Vírus Polimórficos
Têm a capacidade de gerar réplicas de si mesmos utilizando-se de chaves de encriptação diversas, fazendo com que as cópias finais possuam formas diferentes. A polimorfia visa dificultar a detecção de utilitários antivírus, já que as cópias não podem ser detectadas a partir de uma única referência do vírus.

ANALISTA/BACEN/FCC/2005
Um código malicioso que se altera em tamanho e aparência cada vez que infecta um novo programa é um vírus do tipo
(A) de boot.
(B) de macro.
(C) parasita.
(D) camuflado.
(E) polimórfico.

Vírus de Script
São vírus que são executados através de páginas da Web que possuem Scripts interpretados pelo navegador. Sites não confiáveis podem conter códigos maliciosos, os sites de hackers ou outros sites promíscuos são os mais propensos a conterem estes tipos de vírus.

TROJAN HORSE (Cavalo de Tróia)

O Trojan é um programa que age utilizando o princípio do “Cavalo de Tróia”, onde um arquivo é enviado se fazendo passar por um aplicativo útil, como um “presente de grego”, mas que na verdade abre portas de comunicação possibilitando invasões por hackers remotamente.

MP DO RIO GRANDE DO NORTE – CESGRANRIO
Assinale uma alternativa que define um Trojan.
a) São componentes de hardware e software que têm o papel de filtrar as informações da rede, evitando que dados de um sistema sejam acessados sem prévia autorização;
b) conhecido como Cavalo de Tróia, é um arquivo que quando executado abre uma determinada porta do computador, possibilitando acesso total e completo a terceiros;
c) são mensagens de caráter comercial ou promocional não solicitadas enviadas por e-mail;
d) é uma ferramenta utilizada para estabelecer comunicação com outras máquinas em outros lugares;
e) é uma ferramenta que informa se o site a ser acessado tem conexão segura.
Letra B.

WORM
É um programa malicioso que ao infectar uma máquina, não atacam diretamente o computador, tem como característica replicar mensagens sem o consentimento do usuário, espalhando propagandas, arquivos maliciosos ou congestionando a rede.

TST – CESPE – 2008
O termo worm é usado na informática para designar programas que combatem tipos específicos de vírus de computador que costumam se disseminar criando cópias de si mesmos em outros sistemas e são transmitidos por conexão de rede ou por anexos de e-mail.
( ) CERTO ( ) ERRADO
Errado, o worm não combate tipos de vírus!!!

CÂMARA DOS DEPUTADOS – TÉCNICO LEGISLATIVO – FCC – SETEMBRO/2007
Um programa capaz de se auto-propagar automaticamente através de redes, enviando cópias de si mesmo, de computador para computador, denomina-se:
a) Cavalo de Tróia
b) Macro
c) Backup
d) Backdoor
e) Worm
Letra E!

SPYWARE
Um spyware é um programa espião.

PC – ES – CESPE – 2006 – AUXILIAR DE PERÍCIA MÉDICA
Ter receio de se fazer compras on-line ou de se acessar o sítio de um banco pela Internet, justifica-se, atualmente, pela possibilidade de perda de privacidade causada por software maliciosos capazes de enviar dados privativos referentes a senhas de acesso a contas bancárias e números de cartão de crédito a outras máquinas conectadas remotamente na Internet.
( ) Certo ( ) Errado
Certo! Esta questão se refere diretamente aos spywares.

Existem vários programas espiões, os mais relevantes são os Keyloggers que capturam todos os dados digitados pelo usuário e os Screenloggers que capturam telas da área de trabalho do usuário.

ADWARE
O Adware é um software malicioso que insere propagandas em outros programas. Note que não se trata de propagandas nas páginas, mas sim nos próprios navegadores (IE ou Firefox) ou em outros programas em geral.
TRF 1ª REGIÃO – DEZEMBRO/2006 – FCC
Na categoria de códigos maliciosos (Malware), um adware é um tipo de software
A) que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.
B) que tem o objetivo de monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.
C) projetados para apresentar propagandas através de um browser ou de algum outro programa instalado no computador.
D) que permite o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim.
E) capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.

ANTT - NÍVEL MÉDIO - NCE – 2005
Considere as seguintes definições relativas à segurança da informação:
** Adware: programa criado para mostrar propagandas em geral;*
** Cavalo de Tróia: programa que se faz passar por um aplicativo útil, mas possui código malicioso;*
** Spyware: software de segurança desenvolvido para detectar vírus de última geração;*
** Vírus: organismo vivo cuja mutação permite contaminar computadores.*
O número de definições corretas é:
A) 0
B) 1
C) 2
D) 3
E) 4
Letra C! Os dois primeiros itens são verdadeiros.

ROOTKITS
Um rootkit é um conjunto de ferramentas (programas maliciosos) que permitem que crackers acessem a um computador ou rede de computadores.Uma vez que o rootkit é instalado, permite que o atacante ganhe privilégios de root (raiz), ou seja, privilégios de administrador e, possivelmente, o acesso a outras máquinas na rede. Um rootkit pode ser formado de Trojans, Spywares etc.

OUTROS CONCEITOS RELEVANTES

BACKDOOR
É uma brecha, normalmente inserida pelo próprio programador de um sistema para uma invasão. Essa brecha pode ser interessante caso um usuário, por exemplo, esqueça uma senha de acesso, mas ainda assim constitui no mínimo uma vulnerabilidade.

SNIFFER
É um programa utilizado para monitorar as informações em uma rede, "farejadores", originalmente eram usados por administradores de rede, mas quando usados de forma mal-intencionada servem para espionar os dados que trafegam na rede.

PRF – 2003 – CESPE
Para evitar que as informações obtidas em sua pesquisa, ao trafegarem na rede mundial de computadores, do servidor ao cliente, possam ser visualizadas por quem estiver monitorando as operações realizadas na Internet, o usuário tem à disposição diversas ferramentas cuja eficiência varia de implementação para implementação. Atualmente, as ferramentas que apresentam melhor desempenho para a funcionalidade mencionada são as denominadas sniffers e backdoors e os sistemas ditos firewall, sendo que, para garantir tal eficiência, todas essas ferramentas fazem uso de técnicas de criptografia tanto no servidor quanto no cliente da aplicação Internet.
( ) Certo ( ) Errado
Errado! Sniffers e Backdoors???

EXPLOITS
Ferramentas criadas por hackers para permitir explorar vulnerabilidades conhecidas de sistemas e assim permitir que iniciantes (Script Kiddies) possam praticar ações de invasões sem conhecimentos avançados.

ENGENHARIA SOCIAL
Técnica utilizada para obter informações preciosas baseada em uma relação de confiança, onde o agente que a pratica manipula o alvo de alguma forma para obter uma informação. Basicamente é a arte de se contar mentiras de maneira convincente para que atendam aos seus pedidos mesmo que não tenha autoridade para tal.

HONEYPOT
Pote de Mel. Trata-se de uma técnica para atrair um cracker para um determinado lugar e poder, assim, identificar o invasor, por onde ele veio, que comandos ou ferramentas estava utilizado, qual era o alvo, que motivações tem...

INSS – CESPE – MARÇO/2008
O Honeypot é um tipo de software cuja função é detectar ou impedir a ação de agente externo, estranho ao sistema, atraindo-o para outra parte do sistema aparentemente vulnerável.
( ) CERTO ( ) ERRADO
Certo!!!

ROBOT (BOT)
Um bot é um programa que realiza ações repetitivas se fazendo passar por um ser humano. As ações repetitivas podem ser as mais variadas, desde o envio de Spam, a votação em sites que realizam algum tipo de enquete ou ainda ataques de inundação ou congestionamento.
Para evitar a ação dos bots é muito comum que alguns sites criem mecanismos para garantir que aquela ação está de fato sendo praticada por uma pessoa.

CAPTCHAS

Atualmente uma ferramenta comum para evitar a pratica de bots é a CAPTCHA, ela se consiste em uma tela contendo caracteres disformes para visa forçar a visualização de uma confirmação a ser digitada por um ser humano e assim permitir o prosseguimento de uma ação.

CAPTCHA extraída da URL: http://www.receita.fazenda.gov.br/Aplicacoes/ATCTA/cpf/ConsultaPublica.asp

FLOOD
Conceito atribuído ao envio de pacotes de dados repetidos através da rede. Podemos citar como exemplo quando um usuário em um Chat envia a mesma mensagem dezenas de vezes.

TIPOS DE ATAQUES

ATAQUE DE NEGAÇÃO DE SERVIÇO (DoS - Denial of Service)

Um ataque de negação de serviço visa fazer um sistema ou um servidor parar de funcionar (indisponibilidade). Uma maneira de fazer um sistema parar de funcionar pode implicar na utilização de um robot ou um worm, para o envio repetido de pacotes para um servidor.

ANALISTA/BACEN/FCC/2005
Uma DoS ou Denial of Service pode ser provocada por programas maliciosos do tipo:
A) spoofing.
B) spyware.
C) worm.
D) back door.
E) trojan horse.
Letra C!

ATAQUE DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDO (DDoS)
O principal método para realização deste tipo de ataque se consiste em um princípio baseado na telefonia, o congestionamento. Já observaram que no dia 31 de dezembro à meia-noite fica difícil realizar uma ligação devido a uma sobrecarga na rede? Baseado nessa observação um ataque DDoS utiliza máquinas de múltiplas redes para tornar inoperante um serviço. Trata-se de uma variante do ataque DoS mais danosa porque o atacante não é único.

ATAQUES DE FORÇA BRUTA
É a forma de ataque mais básica. Consiste em adivinhar uma senha pelo método de tentativa e erro. Pode utilizar um bot para realizar essa busca exaustiva.

SPOOFING
É um tipo de ataque de rede que tem por objetivo estabelecer uma conexão entre um usuário desconhecido, fazendo-se passar por outro legítimo. Nesse tipo de ataque se

anula um cliente legítimo para assim explorar a relação de confiança obtida e ganhar acessos não autorizados na rede.

PING OF DEATH (Ping da Morte)
Consiste em enviar um pacote TCP/IP com tamanho maior do que o máximo permitido (65535 bytes) para a máquina que deseja atacar, fazendo com que as máquinas travem, reiniciem ou exibam mensagens de erro.

AUDITOR FISCAL DO TRABALHO – ESAF - 2003
Ping da Morte (Ping of Death) é um recurso utilizado na Internet por pessoas mal intencionadas, que consiste
a) no envio de pacotes TCP/IP de tamanho inválidos para servidores, levando-os ao travamento ou ao impedimento de trabalho.
b) na impossibilidade de identificação do número de IP de máquina conectada à rede. Desta forma, muitos dos serviços de segurança disponíveis deixam de funcionar, incluindo os "rastreamentos" que permitem a identificação de segurança das fontes de origem de ataques.
c) em instalar em um computador conectado a uma rede um programa cliente que permite a um programa servidor utilizar esta máquina sem restrições.

d) no mecanismo de "abertura" de portas e acha-se atualmente incorporado em diversos ataques de vírus.
e) na captura e alteração de "pacotes" TCP/IP transmitidos pelas redes.
Letra A!

PHISHING
O Phishing é uma técnica que visa enganar um usuário (fraude), induzindo-o a clicar em um link que o levará para uma página clonada ou um arquivo malicioso.

PHISHING SCAM
O Phishing Scam ocorre quando se recebe o Phishing ao acaso (Scam), de forma aleatória, como por exemplo através de e-mails.

Exemplo de Phishing Scam. Observe que o link direciona para um arquivo com extensão ASP, contido em um site desconhecido.

UFRJ – NCE – JUNHO/2008
Considere a seguinte definição, extraída da Wikipédia:

"é uma forma de fraude eletrônica, caracterizada por tentativas de adquirir informações sensíveis, tais como senhas e números de cartão de crédito, ao se fazer passar por uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial, como um correio ou uma mensagem instantânea".

Essa definição refere-se a:
(A)anti-vírus;
(B) firewall;
(C) phishing;
(D) spam;
(E) vírus.
Letra C!

PHARMING

Na Internet quando se digite o endereço de uma página (URL) em um navegador, é realizada uma consulta em um servidor de nomes de domínios (DNS), no qual é identificado o IP (endereço) da página solicitada e só assim é possível a localização da informação.
O Pharming é um tipo de Phishing, onde o cracker envenena o servidor DNS, alterando os IP's, direcionando os acessos para páginas fraudulentas, com o propósito de capturar informações para um servidor falso, permitindo a ação de golpistas.

AGENTES DE SEGURANÇA

ANTIVÍRUS

Como o nome sugere trata-se de uma ferramenta para remoção dos vírus existentes no computador e combate a entrada novos vírus.

O antivírus deve ser atualizado com a maior freqüência possível, de preferência de forma automática através da Internet, pois a cada dia surgem cerca de 200 novos tipos de vírus.

Alguns exemplos de antivírus cobrados em provas são: McAffe, Norton, AVG, AVAST!, entre outros.

BB – CESPE/2007

Para que um computador esteja efetivamente protegido contra a ação de vírus de computador e contra ataques de hackers, é suficiente que haja, no computador, um programa antivírus que tenha sido atualizado há, no máximo, três meses, sendo desnecessário, atualmente, o uso de firewall no combate a ataques de hackers.

( ) Certo ( ) Errado

Errado! 3 meses sem atualizações tornariam o antivírus ineficaz, outro erro é achar que o antivírus irá substituir a função do Firewall, pois se tratam de ferramentas distintas.

FUND. CULTURAL PARA – CESPE /2007

Vírus é um programa pernicioso, que causa danos nos computadores, apagando ou corrompendo dados. Para se evitar um vírus, deve-se instalar e manter atualizado o

A) Microsoft Office.

B) protocolo TCP/IP.

C) antivírus e o firewall.

D) sistema operacional.

Letra C!

FIREWALL

Um firewall é um dispositivo que protege a rede de ataques externos, ou seja, impede invasões através da Internet. Tal dispositivo pode ser encontrado como Hardware ou Software.

O firewall age também como um filtro, permitindo ou não a passagem das informações que entram e saem da rede. Bem configurado deve trabalhar com regras restritivas, ou seja: TUDO QUE NÃO É PERMITIDO, É PROIBIDO!

POLÍCIA CIVIL – PERITO – FUNIVERSA - MARÇO/2008

Com relação aos dispositivos utilizados em políticas de segurança das organizações relacionadas à área de tecnologia da informação, denominados firewalls e muito úteis para minimizar crimes virtuais, assinale a alternativa correta.

(A) São dispositivos, em forma de software e/ou de hardware, que possuem a função de regular o tráfego de dados entre redes distintas, impedindo a transmissão e/ou a recepção de acessos nocivos ou não autorizados de uma rede para outra.

(B) São dispositivos, em forma de software e/ou de hardware existentes e habilitados no próprio sistema operacional dos computadores, que tem a função de evitar o tráfego de vírus entre computadores de uma mesma rede local, impedindo que tais vírus sejam transmitidos e/ou recebidos de um computador para outro.

(C) São dispositivos em forma de software, não existindo em forma de hardware, que possuem a função de regular o tráfego de dados entre redes distintas, impedindo a transmissão e/ou recepção de acessos nocivos ou não-autorizados de uma rede para outra.
(D) São dispositivos em forma de software, não existindo em forma de hardware, que possuem a função de impedir o tráfego de vírus entre redes distintas, impedindo que tais vírus sejam transmitidos e/ou recebidos de uma rede para outra.
(E) São dispositivos em forma de hardware, não existindo em forma de software, que possuem a função de impedir o tráfego de vírus entre redes distintas, impedindo que tais vírus sejam transmitidos e/ou recebidos de uma rede para outra.
Letra A!

PC – ES – CESPE – 2006 – ESCRIVÃO/DELEGADO/PERITO
Caso situação de espionagem utilizasse recursos de keylogger e armazenasse informações processadas no computador, o uso de sistema firewall seria indicado para impedir que essas informações fossem enviadas a uma máquina de um possível espião na Internet.
( ) Certo ( ) Errado
Certo! Quando o programa espião tentar acessar a rede para enviar a informação indevida o firewall vai constatar que o programa não é permitido e vai bloquear o envio da informação.

PROGRAMAS "ANTI"
Saibam que um bom antivírus tenta combater a maior quantidade de malwares possíveis, mas nem sempre é suficiente. Portanto existem vários programas "anti" com finalidades específicas. O que é importante é compreender que qualquer "anti" específico só combate aquele tipo de praga, logo se cair numa questão que um antispyware combate trojans está errado.
Exemplos de ferramentas de proteção para pragas específicas:

- AntiTrojan
- AntiSpyware
- AntiSpam (Spam não é malware mas observe que existem programas que visam impedir a entrada de propagandas indesejadas na caixa postal do usuário)
- AntiWorm
- AntiPhishing

TÉCNICAS UTILIZADAS PARA GARANTIR A DISPONIBILIDADE

BACKUP
No capítulo de Windows vimos que um backup é uma cópia de segurança que deve ser gravada numa mídia removível em um lugar seguro. Agora precisamos entender de fato como funcionam as rotinas de backup.

Todo arquivo possui um atributo de arquivamento (bit archive) que pode estar marcado (1) ou desmarcado (0). Sempre que salvamos um arquivo esse atributo fica marcado (1).

BACKUP NORMAL/TOTAL/FULL
O backup normal copia todos os arquivos da unidade ou pasta selecionada pelo usuário e retira o atributo de arquivamento (marcando com 0).

BACKUP INCREMENTAL
É utilizado após um backup normal, copiando somente os arquivos que possuem o atributo de arquivamento e retirando tal atributo, portanto copia somente os arquivos novos e alterados gerando um arquivo que será acrescido ao backup normal e assim sucessivamente. Logo, se um usuário cria um backup normal no dia 1 e incrementais a cada dia posterior se der um problema no dia 6 ele terá que recuperar o arquivo do dia 1 (normal) e os arquivos incrementais dos dias 2, 3, 4 e 5 em seqüência.

BACKUP DIFERENCIAL
É utilizado após um backup normal, copiando somente os arquivos que possuem o atributo de arquivamento mas NÃO retira tal atributo, portanto copia somente os arquivos novos e alterados gerando um arquivo que irá acumular todas as atualizações desde o último backup normal ou incremental. Logo, se um usuário cria um backup normal no dia 1 e diferenciais a cada dia posterior se der um problema no dia 6 ele terá que recuperar o arquivo do dia 1 (normal) e o arquivos diferencial do dia 5, descartando os diferenciais anteriores.

BACKUP DE CÓPIA
O backup de cópia, como o nome diz, copia todos os arquivos da unidade ou pasta selecionada pelo usuário e não retira o atributo de arquivamento (marcando com 0), ou seja pode ser utilizado sem alterar uma rotina de backup já existente.

BACKUP DIÁRIO
Não se importa com o atributo de arquivamento, tendo como único critério a data de criação ou modificação do arquivo.

ELETROBRAS – NCE
Um usuário doméstico utiliza a ferramenta de backup do MS Windows 2000 para manter uma cópia segura dos seus dados em um HD removível. Ele utiliza a seguinte política de backup:
• todo dia 7 de cada mês: backup normal
• todo dia 14 de cada mês: backup incremental
• todo dia 21 de cada mês: backup incremental
• todo dia 28 de cada mês: backup diferencial
Suponha que, ao ligar o seu computador, no dia 22, esse usuário perceba que seu disco foi corrompido. Para ter seus dados de volta, os backups que ele deve restaurar, na ordem correta, são:
(A) o backup do dia 21, o backup do dia 14, o backup do dia 7;
(B) o backup do dia 7 e o backup do dia 21;
(C) o backup do dia 7, o backup do dia 14, o backup do dia 21;
(D) somente o backup do dia 21;
(E) somente o backup do dia 7.
Letra C!

ESPELHAMENTO DE DISCOS (RAID-1)
O espelhamento de discos é tolerante a falhas e fornece redundância de dados usando duas cópias, ou espelhos, para duplicar os dados nele armazenados. Cada espelho se consiste em um disco, o que é gravado em um é gravado simultaneamente no outro. O espelhamento também é conhecido como RAID 1.

Se um dos discos físicos falhar, os dados no disco com falha ficarão indisponíveis, mas o sistema continuará a funcionar usando o disco não afetado automaticamente.

TÉCNICA UTILIZADA PARA GARANTIR A CONFIDENCIALIDADE

CRIPTOGRAFIA DE CHAVE SECRETA (SIMÉTRICA)

CRIPTOANÁLISE

CRIPTOGRAFIA DE CHAVE PÚBLICA (ASSIMÉTRICA)

ESTEGANOGRAFIA

TÉCNICA UTILIZADA PARA GARANTIR A INTEGRIDADE

FUNÇÃO HASH

TÉCNICA UTILIZADA PARA GARANTIR A AUTENTICIDADE

SENHAS
BIOMETRIA
CERTIFICAÇÃO DIGITAL

PSI (Política de Segurança da Informação)

Termo de Compromisso

Uma política de segurança é um conjunto de diretrizes que definem formalmente as regras e os direitos dos funcionários, prestadores de serviços e demais usuários, visando à proteção adequada dos ativos da informação. Tal política deve ser garantida pela aplicação formal de um termo de compromisso.