SEGURANÇA DA INFORMAÇÃO VII

2. SPAM

O spam é um e-mail enviado indevidamente, geralmente para um grande número de pessoas, sem autorização. Ele pode ter um propósito comercial, por exemplo.

FORMAS DE PREVENÇÃO

O usuário tem um papel ativo em relação à segurança. Mesmo possuindo o melhor antivírus, ele deve se atentar para não clicar em links duvidosos.

SENHAS

- Nunca compartilhar as senhas;
- Alterá-las regularmente;
- Sempre que possível, usar autenticação em duas etapas;

Em alguns aplicativos, como o e-mail, por exemplo, além da senha de acesso, existe a autenticação multifator, que é única para cada autenticação, gerando um código aleatório. Esse método trata-se de uma segunda camada de proteção. Muitas pessoas caem em golpes no WhatsApp ao vender um produto em plataformas de vendas online. O atacante entra em contato dizendo que precisa verificar a conta e pede a confirmação de um código. Em certos casos, as pessoas não percebem que o código é do WhatsApp, permitindo que o atacante tenha acesso ao aplicativo.

- Não usar a mesma senha para diversos contextos;

Não é recomendável usar a mesma senha para diversos contextos. Isso porque, uma vez capturada, o atacante tentará fazer a autenticação com a mesma senha em outros serviços.

Obs.: Existe uma distância entre o que é recomendado e o que é realizado na prática. Na prova, o candidato deve se atentar e aplicar a teoria.

- Não usar informações dedutíveis (nome, data nascimento etc.);
- Não usar senhas curtas.

Vários meios recomendam o uso de senhas com oito caracteres, misturando letras maiúsculas e minúsculas, números e caracteres especiais. No entanto, isso não é algo que pode ser levado para a prova como regra.

5m

ANTIVÍRUS

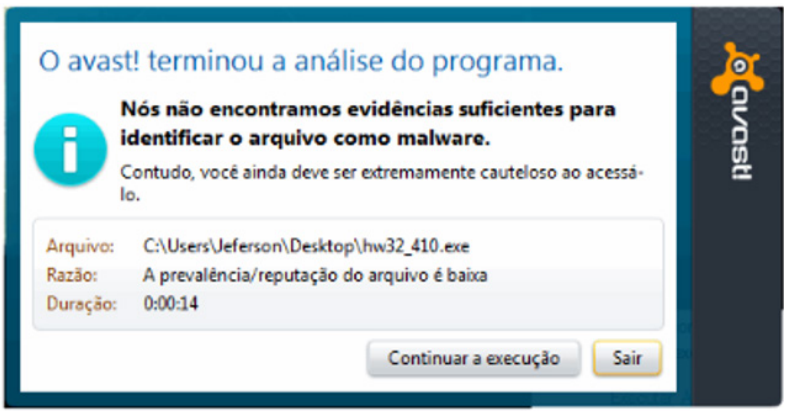
O antivírus é uma proteção contra diversos tipos de ameaças, inclusive malwares. Em tese, existe uma proteção específica para cada tipo de ameaça. Por exemplo, há programas anti-spywares que detectam apenas spywares. Geralmente, as empresas oferecem antivírus com proteção genérica, que inclui vários tipos de proteção.

O objetivo do antivírus é detectar e eliminar ameaças. No entanto, isso não significa que ele fará isso necessariamente. A regra do antivírus é detectar e eliminar ameaças que ele conhece. Por isso, é necessária a atualização constante do antivírus, uma vez que novas ameaças estão surgindo a todo momento. Essas ameaças são descobertas e analisadas, e uma vacina é criada para elas. Esse processo leva um tempo, durante o qual as ameaças estão circulando e podem invadir a máquina.

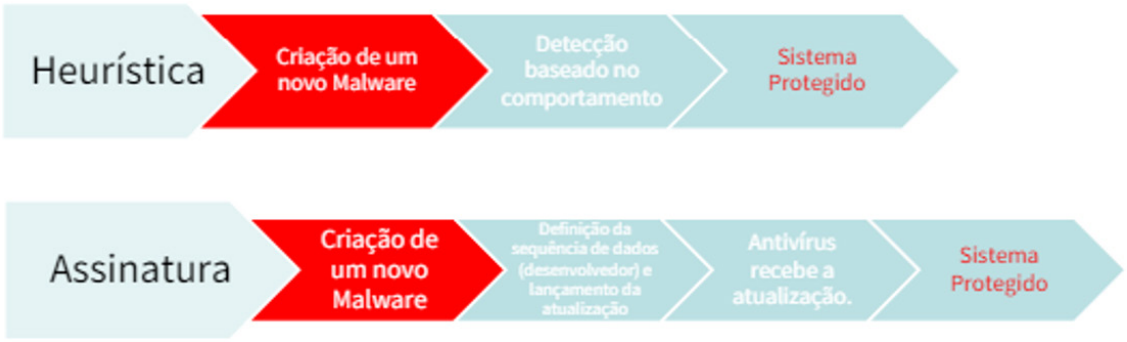
Entre o surgimento de uma ameaça e a identificação eficaz dela, existe um processo chamado heurística, que detecta ameaças com base no comportamento anômalo dos arquivos. Se um arquivo faz algo que não é padrão, ele é verificado pelo antivírus. Vale ressaltar que essa verificação pode gerar dois problemas: o falso positivo, em que um programa é detectado como uma ameaça quando na verdade não é, e ele é suspenso; e o falso negativo, em que um programa não parece ser uma ameaça e é executado normalmente, contaminando a máquina. Todavia, mesmo com esses riscos, pode ocorrer uma detecção correta.

10m

HEURÍSTICA



ANTIVÍRUS (ANTIMALWARE)



Obs.: Nem a heurística nem a assinatura trazem total proteção.

FIREWALL

O firewall é um sistema que monitora as conexões de entrada e saída de uma máquina na rede, bloqueando o que não é permitido e permitindo o tráfego autorizado. Esse sistema se baseia nas regras cadastradas no firewall, também conhecidas como políticas de segurança aplicadas ao firewall. É importante destacar que podem ocorrer erros nesse sistema, permitindo a passagem de algo indevido que pode contaminar a máquina.

Obs.: não há como garantir total proteção, mesmo utilizando todos os softwares do mundo. Além disso, quanto maior o nível de proteção, pode-se comprometer o desempenho. Firewalls muito avançados e verificações intensas tornam o tráfego na rede quase impossível, sendo necessário encontrar um equilíbrio dependendo do contexto.

DIRETO DO CONCURSO

19. (2024/ADM TEC/PREFEITURA DE PALMEIRA DOS ÍNDIOS/TÉCNICO EM REDES DE COMPUTADORES) Analise as informações a seguir:

I – Fraude bancária online é um dos crimes cibernéticos mais comuns no Brasil, cometido quase sempre pelo Phishing, quando o criminoso finge ser instituição financeira legítima para conseguir dados pessoais e financeiros da vítima.
II – O crime cibernético denominado de ciberstalking ocorre quando o criminoso bloqueia o acesso do usuário a seus próprios dados para chantagear pagamento como condição para devolver o acesso. Geralmente é cometido contra empresas e usuários individuais abastados, provocando transtornos financeiros.
III – Um tipo de cibercrime que afeta o aspecto emocional da vítima é o Ransomware. Ele consiste no assédio online com perseguições, ameaças ou cerco de intimidação contra alguém. É um crime que causa graves danos emocionais para a vítima e com difícil possibilidade de identificação e punição do autor.

Marque a alternativa CORRETA:
a. Todas as afirmativas estão corretas.
b. Nenhuma afirmativa está correta.
c. Apenas uma afirmativa está correta.
d. Apenas duas afirmativas estão corretas

Obs.: O candidato não precisa se preocupar com as estatísticas. Essa análise cabe ao examinador.

15m

II – Cyberstalking é quando uma pessoa persegue virtualmente alguém que não deseja ter contato com ela.
III – Na verdade, trata-se de cyberstalking.

20. (2024/CEBRASPE/CNPQ/ANALISTA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO) Cavalo de Troia de acesso remoto é um programa que permite ao atacante acessar remotamente o equipamento da vítima e executar ações como se fosse o usuário legítimo, combinando, assim, as características de cavalo de Troia e backdoor.

O cavalo de Troia de acesso remoto é o RAT.

21. (2024/FUNDEP GESTÃO DE CONCURSOS FUNDEP/TÉCNICO EM LABORATÓRIO) Relacione os tipos de ataques cibernéticos listados na COLUNA I com as características correspondentes na COLUNA II.

COLUNA I

1. Engenharia social
2. Força bruta

COLUNA II

( ) Baseia-se na manipulação psicológica das pessoas para obter informações confidenciais ou acesso a sistemas.
( ) Concentra-se em quebrar senhas, chaves criptográficas ou outros mecanismos de segurança por meio de tentativas repetitivas e automatizadas.
( ) Os atacantes exploram a confiança, a curiosidade ou a ingenuidade das vítimas para alcançar seus objetivos.

Assinale a sequência correta.
a. 2 1 1
b. 1 2 2
c. 2 2 1
d. 1 2 1

---

22. (2024/CEBRASPE/CNPQ/ANALISTA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO) Um vírus de computador tem a capacidade de se disseminar automaticamente, sem a necessidade de uma ação humana.

O vírus precisa ser executado, requerendo a ação humana para que ele se propague.

---

23. (2024/INSTITUTO VERBENA/TJ-AC/ANALISTA JUDICIÁRIO) Códigos maliciosos ou malwares são programas de computador idealizados para causar danos nos sistemas computacionais ou exfiltrar dados dos mesmos. O malware que tem a capacidade de propagar-se automaticamente pelas redes, promovendo a exploração de vulnerabilidades nos sistemas e aplicativos e, ainda, enviando cópias de si mesmo de um dispositivo para outro é o:

a. vírus.
b. adware.
c. ransomware.
d. worm.

Exfiltrar significa retirar dados de dentro de um sistema.
a. O vírus não tem essa capacidade.
b. O adware é um tipo de spyware que exibe propagandas.
c. O ransomware criptografa os dados e pede resgate.

---

24. (2024/FGV/PREFEITURA DE SÃO JOSÉ DOS CAMPOS/TÉCNICO TRIBUTÁRIO) Considere as seguintes afirmativas acerca de técnicas e aplicativos de segurança:

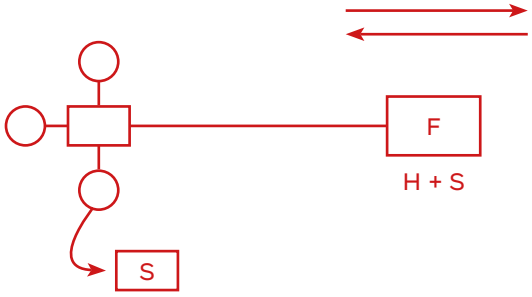
20m

I – Um programa antivírus bloqueia o acesso de usuários não autorizados ao computador local e adicionalmente pode determinar quais formatos de senha são seguros para serem utilizados.
II – Um firewall analisa o tráfego de rede para determinar quais operações de entrada e saída podem ser executadas, a partir de um conjunto de regras.
III – Um firewall pode ser um aplicativo de software executando em um computador local.

Está correto o que se afirma em

a. I e II, apenas.
b. II e III, apenas.
c. III, apenas.
d. I, apenas.
e. I, II e III.

I – O papel dos antivírus é detectar e eliminar ameaças.
II – O firewall pode ser apenas um software, mas também pode ser uma combinação de software e hardware. Esta última é mais comum para firewalls de rede, que consiste em uma rede com vários computadores conectados que se conecta a outra rede com um firewall. Já o firewall que é de apenas um software, protege apenas a máquina e não toda a rede.
O firewall de rede (software + hardware) filtra o tráfego que entra e sai. Pode ser implementado por meio de dispositivos ou outros sistemas e faz um filtro do que pode ser acessado, incluindo sites.

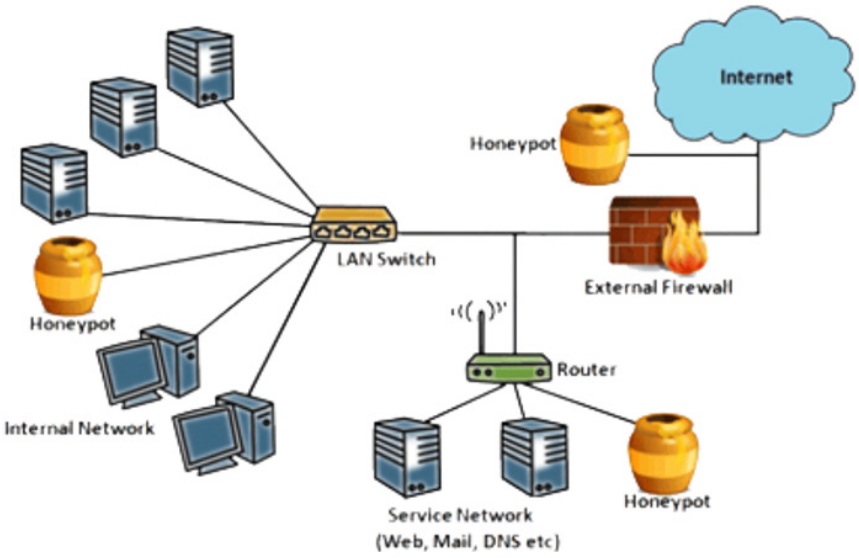


OUTRAS PROTEÇÕES

ESTEGANOGRAFIA

A esteganografia é uma técnica de esconder uma mensagem em uma imagem ou até mesmo em um vídeo.

HONEYPOT



Os honeypots são computadores deixados na rede com o objetivo de parecerem computadores normais, facilitando o acesso sem que o atacante perceba. É como uma casa com alguns cômodos extremamente trancados e outros mais fáceis de serem acessados. Quando um honeypot na rede é acessado, o atacante passa a ser monitorado e detectado.

TOKEN

O token é um dispositivo usado para fazer login. Ele pode substituir a senha ou ser utilizado como parte de uma autenticação de múltiplos fatores, como uma segunda senha ou um código necessário.

25m

CARTÃO INTELIGENTE – SMARTCARD

O cartão inteligente contém um chip que armazena dados para autenticação. O problema do smartcard, e até mesmo do token, é que eles podem ser furtados.

GABARITO

19. c

20. C

21. d

22. E

23. d

24. b