TECNOLOGIA DA INFORMAÇÃO

Segurança da Informação – Parte I

Livro Eletrônico

GRAN CURSOS ONLINE

SUMÁRIO

Apresentação

À luta, guerreiro(a)! É um prazer revê-lo(a).

Confiança é um dos grandes segredos do **sucesso**. Estude com dedicação, trabalhe duro (quem disse que seria moleza!), faça com direção, foco, siga as dicas que fornecemos durante o curso e, com certeza, terá mais soldados a seu favor e **sucesso total nesta batalha** que se aproxima☺***!***

Rumo então à aula sobre **Segurança da Informação (Parte I)**.

Que Deus o(a) abençoe e sucesso nos estudos!

SEGURANÇA DA INFORMAÇÃO – PARTE I

1. O Contexto Atual

A Segurança da Informação é um assunto de grande importância na atualidade e tem sido alvo de atenção por parte das organizações.

Mas, o que significa **segurança**?

É colocar tranca nas portas de sua casa? É ter as informações guardadas de forma suficientemente segura para que pessoas sem autorização não tenham acesso a elas? **Vamos nos preparar para que a próxima vítima não seja você!**

A **segurança** é uma palavra que está presente em nosso cotidiano e refere-se a um estado de proteção, em que estamos "livres" de perigos e incertezas!

Obs.: **segurança da informação** é o processo de proteger a informação de diversos tipos de **ameaças externas e internas** para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.

Em uma corporação, a segurança está ligada a tudo o que manipula direta ou indiretamente a informação (**inclui-se aí também a própria informação e os usuários**) e que merece proteção. Esses elementos são chamados de **ATIVOS** e podem ser divididos em:

- **Tangíveis**: informações impressas, móveis, hardware (Ex.: impressoras, scanners);
- **Intangíveis**: marca de um produto, nome da empresa, confiabilidade de um órgão federal etc.;
- **Lógicos**: informações armazenadas em uma rede, sistema ERP (Sistema de Gestão Integrada) etc.;
- **Físicos**: galpão, sistema de eletricidade, estação de trabalho etc.;
- **Humanos**: funcionários.

Para Beal (2005), **ativo de informação** é qualquer dado ou informação a que esteja associado um valor para o negócio. Representam ativos de informação as informações relevantes

mantidas na mente dos tomadores de decisão, em base de dados, arquivos de computador, documentos e planos registrados em papel etc.

Segundo Technet (2006) um **ativo** é "todo elemento que compõe o processo da comunicação, partindo da informação, seu emissor, o meio pelo qual é transmitida, até chegar ao seu receptor".

Moreira (2001, p.20) afirma que:

> [...] **ativo** é tudo que manipula direta ou indiretamente uma informação, inclusive a própria informação, dentro de uma Organização e, é isso que deve ser protegido contra **ameaças** para que o negócio funcione corretamente. **Uma alteração, destruição, erro ou indisponibilidade de algum dos ativos pode comprometer os sistemas e, por conseguinte, o bom funcionamento das atividades de uma empresa**.

De acordo com a NBR ISO/IEC 27002: 2005, a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser **adequadamente protegida**.

A informação pode existir em diversas formas: pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Dessa definição, podemos depreender que **a informação é um bem, um patrimônio a ser preservado para uma empresa e que tem importância aos negócios**. Devido a essa importância, deve ser oferecida proteção adequada, ou seja, **a proteção deve ser proporcional à importância que determinada informação tem para uma empresa.**

Soluções pontuais isoladas não resolvem toda a problemática associada à segurança da informação. **Segurança se faz em pedaços, porém todos eles integrados**, como se fossem uma corrente.

Segurança se faz protegendo todos os elos da corrente, ou seja, todos os ativos (físicos, tecnológicos e humanos) que compõem seu negócio. Afinal, o poder de proteção da corrente está diretamente associado ao elo mais fraco!

2. Princípios da Segurança da Informação

A segurança da informação busca proteger os **ativos** de uma empresa ou indivíduo com base na preservação de alguns **princípios**. Vamos ao estudo de cada um deles.

Os três **princípios** considerados centrais ou principais, mais comumente cobrados em provas, são:

- **confidencialidade;**
- **integridade;**
- **disponibilidade.**

Eles formam aquilo que chamamos de pirâmide ou **tríade da Segurança da Informação** (É possível encontrar a sigla **CID,** para fazer menção a esses princípios!).

Confidencialidade (ou Sigilo): é a **garantia de que a informação não será conhecida por quem não deve.** O acesso às informações deve ser limitado, ou seja, somente as pessoas explicitamente autorizadas podem acessá-las. **Perda de confidencialidade significa perda de segredo.** Se uma informação for confidencial, ela será secreta e deverá ser guardada com segurança, e não divulgada para pessoas sem a devida autorização para acessá-la.

A CONFIDENCIALIDADE busca:

- **proteção contra exposição não autorizada;**
- **acesso somente por pessoas autorizadas.**

Exemplo: o número do seu cartão de crédito só poderá ser conhecido por você e pela loja em que é usado. Se esse número for descoberto por alguém mal-intencionado, o prejuízo causado pela perda de confidencialidade poderá ser elevado, já que poderão se fazer passar por você para realizar compras pela Internet, proporcionando-lhe prejuízos financeiros e uma grande dor de cabeça.

Integridade: destaca que a informação deve ser mantida na condição em que foi liberada pelo seu proprietário, garantindo a sua proteção contra mudanças intencionais, indevidas ou acidentais. Em outras palavras, **é a garantia de que a informação que foi armazenada é a que será recuperada!**

A INTEGRIDADE busca:

- **proteção contra codificação não autorizada;**
- **modificação somente pelas partes devidamente autorizadas.**

A quebra de integridade pode ser considerada sob dois aspectos:

- **Alterações nos elementos que suportam a informação** - são feitas **alterações na estrutura física e lógica em que uma informação está armazenada.** Por exemplo, quando são alteradas as configurações de um sistema para ter acesso a informações restritas;
- **Alterações do conteúdo dos documentos;**

Exemplos: imagine que alguém invada o *notebook* que está sendo utilizado para realizar a sua declaração do Imposto de Renda deste ano, e, momentos antes de você enviá-la para a Receita Federal a mesma é alterada sem o seu consentimento! Neste caso, a informação não será transmitida da maneira adequada, o que quebra o princípio da integridade.
Alteração de *sites* por *hackers*.

- **Disponibilidade**: é a garantia de que a informação deve estar disponível, sempre que seus usuários (pessoas e empresas autorizadas) necessitarem, não importando o motivo. Em outras palavras, é a garantia que a informação sempre poderá ser acessada!

A DISPONIBILIDADE busca acesso disponível às **entidades autorizadas** sempre que **necessário**.

Exemplo: quebra do princípio da disponibilidade quando você decidir enviar a sua declaração do Imposto de Renda pela Internet, no último dia possível, e o *site* da Receita Federal estiver indisponível.

Esses princípios são aplicados na prática, nos ambientes tecnológicos, a partir de um conjunto de **controles** como, por exemplo, criptografia, autenticação de usuários e **equipamentos redundantes** (possui um segundo dispositivo que está imediatamente disponível para uso quando da falha do dispositivo principal).

O que queremos sob a ótica de segurança?

Desejamos entregar **a informação CORRETA, para a pessoa CERTA, no MOMENTO EM QUE ELA FOR NECESSÁRIA!**

Entendeu?

Eis a essência da aplicação dos três princípios aqui já destacados. Ainda, cabe destacar que **a perda de pelo menos um desses princípios já irá ocasionar impactos ao negóc**io (aí surgem os **INCIDENTES**[1] **de segurança**).

Obs.: quando falamos em segurança da informação, estamos nos referindo a **salvaguardas para manter a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente!**

Outros **princípios (**ou **aspectos)** podem ainda ser também levados em consideração, como por exemplo:

- **Autenticidade:** é a propriedade que **garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.** Refere-se à atribuição apropriada do proprietário ou criador dos dados;

(CESPE/SEFAZ-RS/AUDITOR-FISCAL DA RECEITA ESTADUAL - BLOCO I/2019) Para o estabelecimento de padrões de segurança, um dos princípios críticos é **a necessidade de se verificar a legitimidade de uma comunicação, de uma transação ou de um acesso a algum serviço.** Esse princípio refere-se à **Autenticidade**.

[1] **Incidente de segurança da informação**: é indicado por um **simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança**. Exemplos: invasão digital; violação de padrões de segurança de informação.

- **Não repúdio (ou irretratabilidade): é a garantia de que um agente não consiga negar (dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação.** Tal garantia é condição necessária para a validade jurídica de documentos e transações digitais. Só se pode garantir o não repúdio quando houver **autenticidade** e **integridade** (ou seja, quando for possível determinar quem mandou a mensagem e garantir que a mesma não foi alterada).

NÃO REPÚDIO:

- **Proteção contra negação de envio (ou recepção) de determinada informação;**
- **Confiabilidade:** pode ser caracterizada como a **condição em que um sistema de informação presta seus serviços de forma eficaz e eficiente**, ou melhor, um sistema de informação irá "desempenhar o papel que foi proposto para si".

CONFIABILIDADE:

- Visa garantir que um sistema vai se comportar (vai realizar seu serviço) segundo o esperado e projetado **("ser confiável", "fazer bem seu papel");**
- **Auditoria**: é a **possibilidade de rastrear o histórico dos eventos de um sistema** para determinar quando e onde ocorreu uma violação de segurança, bem como identificar os envolvidos nesse processo;
- **Legalidade:** aderência do sistema à **legislação**.
- **Privacidade:** diz respeito ao direito fundamental de cada indivíduo de decidir quem deve ter acesso aos seus dados pessoais. **A privacidade é a capacidade de um sistema manter incógnito um usuário** (capacidade de um usuário realizar operações em um sistema sem que seja identificado), **impossibilitando a ligação direta da identidade do usuário com as ações por este realizadas**. Privacidade é uma característica de segurança requerida, por exemplo, em eleições secretas.

Uma informação privada deve ser vista, lida ou alterada somente pelo seu dono. **Esse princípio difere da confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada.**

3. Vulnerabilidades de Segurança

Vulnerabilidade é uma **fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque.**

Pode ser entendida também como uma **evidência** ou **fragilidade** que eleva o grau de exposição dos ativos que sustentam o negócio, aumentando a probabilidade de sucesso pela investida de uma ameaça.

Ainda, trata-se de **falha no projeto, implementação ou configuração de software ou sistema operacional** que, quando explorada por um atacante, resulta na violação da segurança de um computador.

O conhecimento do maior número de vulnerabilidades possíveis permite à equipe de segurança tomar **medidas para proteção**, evitando assim ataques e consequentemente perda de dados.

Não há uma receita ou lista padrão de vulnerabilidades. Esta deve ser levantada junto a cada organização ou ambiente. Sempre se deve ter em mente o que precisa ser protegido e de quem precisa ser protegido de acordo com as ameaças existentes. Podemos citar, como exemplo inicial, uma análise de ambiente em uma sala de servidores de conectividade e Internet com a seguinte descrição: **a sala dos servidores não possui controle de acesso físico. Eis a vulnerabilidade detectada nesse ambiente.**

Outros exemplos de **vulnerabilidades**:

- ambientes com informações sigilosas com acesso não controlado;
- falta de mecanismos de monitoramento e controle (auditoria);
- inexistência de políticas de segurança;
- ausência de recursos para combate a incêndios;
- hardware sem o devido acondicionamento e proteção;
- falta de atualização de software e hardware;
- ausência de pessoal capacitado para a segurança;
- instalações prediais fora do padrão etc.

4. Ameaças à Segurança da Informação

Ameaça é algo que possa provocar **danos** à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio, mediante a exploração de uma determinada **vulnerabilidade**.

Em outras palavras, uma **AMEAÇA é tudo aquilo que pode comprometer a segurança de um sistema, podendo ser acidental** (falha de hardware, erros de programação, desastres naturais, erros do usuário, bugs de software, uma ameaça secreta enviada a um endereço incorreto etc.) **ou deliberada** (roubo, espionagem, fraude, sabotagem, invasão de hackers, entre outros).

Ameaça pode ser uma **pessoa**, uma **coisa**, um **evento** ou uma ideia capaz de causar dano a um recurso, em termos de confidencialidade, integridade, disponibilidade etc.

Basicamente existem **dois tipos de ameaças**: **internas** e **externas**.

Ameaças externas: representadas por todas as tentativas de ataque e desvio de informações vindas de fora da empresa. Normalmente, essas tentativas são realizadas por pessoas com a intenção de prejudicar a empresa ou para utilizar seus recursos para invadir outras empresas.

Ameaças internas: estão presentes, independentemente das empresas estarem ou não conectadas à Internet. Podem causar desde incidentes leves até os mais graves, como a inatividade das operações da empresa.

Como **exemplos de ameaças** podemos destacar: concorrente, cracker, erro humano (deleção de arquivos digitais acidentalmente etc.), acidentes naturais (inundação etc.), funcionário insatisfeito, técnicas (engenharia social etc.), ferramentas de software (sniffer, cavalo de troia etc.).

Obs.: **os ATIVOS são os elementos que sustentam a operação do negócio e estes sempre trarão consigo VULNERABILIDADES que, por sua vez, submetem os ativos a AMEAÇAS.**

5. Risco

Risco é a medida da exposição à qual o sistema computacional está sujeito. Depende de a probabilidade de uma ameaça atacar o sistema e do impacto resultante desse ataque.

Sêmola (2003, p. 50), diz que **risco é a "probabilidade de ameaças explorarem vulnerabilidades, provocando *perdas de confidencialidade, integridade* e disponibilidade, causando, possivelmente, impactos nos negócios".**

Exemplo de um **risco** pode-se imaginar um funcionário insatisfeito e um martelo ao seu alcance; nesse caso o funcionário poderia danificar algum ativo da informação.

Existem algumas maneiras de se classificar o grau de risco no mercado de segurança, mas de uma forma simples, poderíamos tratá-lo como **alto, médio e baixo risco**.

No caso do nosso exemplo da sala dos servidores, poderíamos dizer que, baseado na vulnerabilidade encontrada, a ameaça associada é de alto risco.

6. Ciclo da Segurança

Como mostrado na figura seguinte, os **ATIVOS** de uma organização precisam ser protegidos, pois estão sujeitos a **VULNERABILIDADES.**

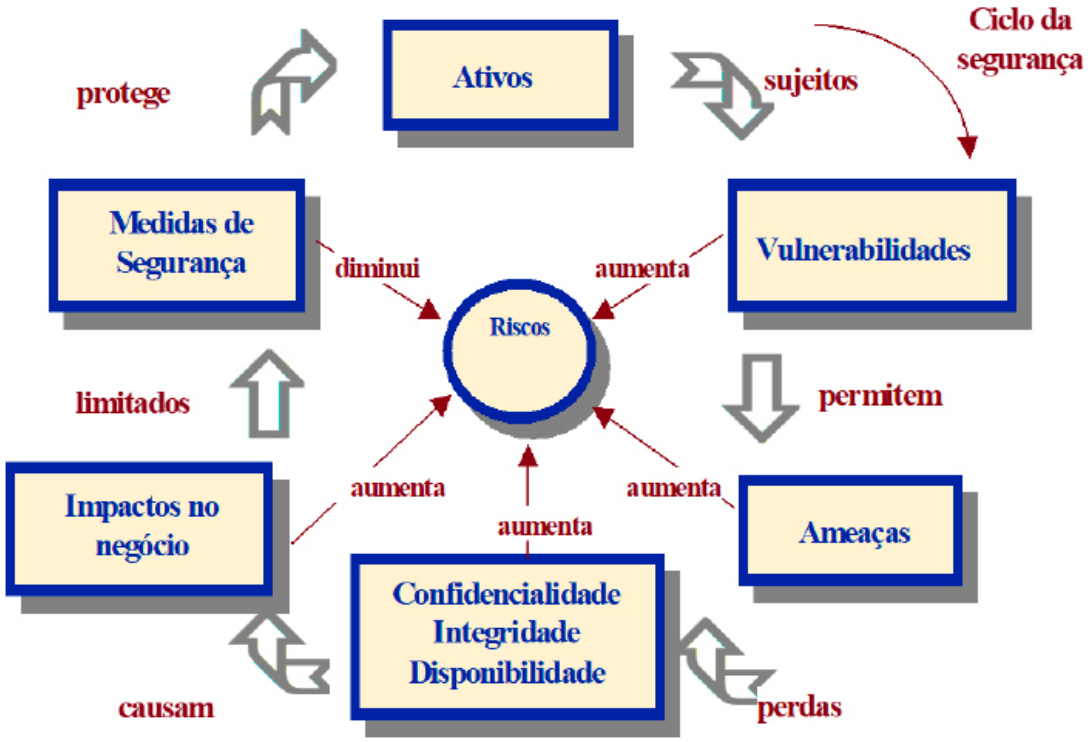


Figura. Ciclo da Segurança da Informação (MOREIRA, 2001)

Se as vulnerabilidades aumentam, aumentam-se os riscos permitindo a exploração por uma ameaça e a concretização de um ataque. Se estas ameaças crescem, aumentam-se ainda mais os riscos de perda da integridade, disponibilidade e confidencialidade da informação, podendo causar impacto nos negócios.

Nesse contexto, **MEDIDAS DE SEGURANÇA** devem ser tomadas, os riscos devem ser analisados e diminuídos para que se estabeleça a segurança dos ativos da informação.

As ameaças são causas em potencial de um incidente indesejado (por exemplo, um ataque de um hacker é uma ameaça). As ameaças e as vulnerabilidades aumentam os riscos relativos à segurança por parte de uma organização.

Dessa forma, podemos dizer que os **riscos** são medidos pela **combinação** entre:

- **número de vulnerabilidades** dos ativos;
- a **probabilidade** de vulnerabilidades serem exploradas por uma ameaça; e
- o **impacto** decorrente dos incidentes de segurança na organização.

6.1. Noções de Vírus, Worms e outras Pragas virtuais

Você sabe o significado de malware?

Obs.: | **malware** (combinação de malicious software – programa malicioso)!

Malware é um termo genérico, usado para todo e quaisquer softwares maliciosos, programados com o intuito de prejudicar os sistemas de informação, alterar o funcionamento de programas, roubar informações, causar lentidões de redes computacionais, dentre outros.

Resumindo, **malwares** são programas que executam deliberadamente ações mal-intencionadas em um computador.

Certbr (2012) destaca algumas das diversas maneiras como os códigos maliciosos (malwares) podem infectar ou comprometer um computador. São elas:

- por meio da **exploração de vulnerabilidades** (falhas de segurança), existentes nos programas instalados;
- por meio da **autoexecução de mídias removíveis infectadas**, como pendrives;
- pelo **acesso a páginas da Web maliciosas**, com a utilização de navegadores vulneráveis;

- por meio da **ação direta de atacantes** que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela **execução de arquivos previamente infectados**, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.

São **espécies de *malware***:

- **vírus;**
- **worms;**
- **bots;**
- **cavalos de troia (trojans);**
- **ransomwares;**
- **spyware;**
- **keylogger;**
- **screenlogger;**
- **backdoors;**
- **rootkits etc.**

Vírus

São pequenos códigos de programação maliciosos que se "agregam" a arquivos e são transmitidos com eles. Trata-se de um **programa (ou parte de um programa)** que se anexa a um arquivo de programa qualquer (como se o estivesse "parasitando") e depois disso procura fazer cópias de si mesmo em outros arquivos semelhantes.

Quando o arquivo é aberto na memória RAM, o vírus também é, e, a partir daí se **propaga** infectando, isto é, inserindo cópias de si mesmo e se **tornando parte de outros programas e arquivos de um computador.**

O **vírus depende da execução do programa ou arquivo hospedeiro** para que possa se tornar ativo e dar continuidade ao processo de infecção. Alguns vírus são inofensivos, outros, porém, podem danificar um sistema operacional e os programas de um computador.

A seguir, destacamos alguns arquivos que podem ser **portadores de vírus de computador**:

- **Arquivos executáveis**: com extensão.exe ou.com; arquivos de scripts (outra forma de executável): extensão.vbs;
- **Atalhos**: extensão.lnk ou.pif; **proteção de tela** (animações que aparecem automaticamente quando o computador está ocioso): extensão.scr;
- **Documentos do MS-Office**: como os arquivos do Word (extensão.doc,.docx,.dot, etc.), arquivos do Excel (.xls,.xlsx,.xlt, etc.), apresentações do Powerpoint (.ppt,.pptx,.pps, etc.), bancos de dados do Access (.mdb, etc.). Arquivos multimídia do Windows Media Player: músicas com extensão.WMA, vídeos com extensão.WMV, dentre outros.

Dentre os **principais TIPOS de vírus** merecem destaque:

Vírus Polimórficos	**Alteram seu formato ("mudam de forma") constantemente.** A cada nova infecção, esses vírus geram uma nova sequência de bytes em seu código, para que o antivírus se confunda na hora de executar a varredura e **não** reconheça o invasor.
Vírus Oligomórfico	**Usa a criptografia** para se defender sendo capaz de alterar também a rotina de criptografia em um número de vezes pequeno. Um vírus que possui duas rotinas de criptografia é então classificado como oligomórfico (LUPPI, 2006).
Vírus de Setor de Carga (Boot Setor) ou Vírus de *Boot*	**Infectam o setor de *boot*** (ou MBR – Master Boot Record – Registro Mestre de Inicialização) **dos discos rígidos.** Obs.: o **Setor de Boot** do disco rígido é a primeira parte do disco rígido que é lida quando o computador é ligado. Essa área é lida pelo **BIOS** (programa responsável por "acordar" o computador) a fim de que seja encontrado o Sistema Operacional (o programa que vai controlar o computador durante seu uso).

Vírus de Macro	Vírus que **infectam documentos que contém macros** (conjunto de comandos que são armazenados em alguns aplicativos e utilizados para automatizar tarefas repetitivas). Um exemplo seria, em um editor de textos, definir uma **macro** que contenha a sequência de passos necessários para imprimir um documento, com a orientação de retrato, e utilizando a escala de cores em tons de cinza. **Um vírus de macro é escrito de forma a explorar esta facilidade de automatização e é parte de um arquivo que normalmente é manipulado por algum aplicativo que utiliza macros**. Para que o vírus possa ser executado, o arquivo que o contém precisa ser aberto e, a partir daí, o vírus pode executar uma série de comandos automaticamente e infectar outros arquivos no computador. Existem alguns aplicativos que possuem **arquivos base** (**modelos**) que são abertos sempre que o aplicativo é executado. Caso este arquivo base seja infectado pelo vírus de macro, toda vez que o aplicativo for executado, o vírus também será. **Arquivos nos formatos gerados por programas da Microsoft, como o Word, Excel, Powerpoint e Access são os mais suscetíveis a este tipo de vírus.** Arquivos nos formatos RTF, PDF e PostScript são menos suscetíveis, mas isso não significa que não possam conter vírus.
Vírus de Macro	 Normal.dot Modelo do Microsoft Word 14 KB Normal.dot–Principal alvo de vírus de macro p/Word
Vírus de Programa	**Infectam arquivos de programa** (de inúmeras extensões, como.exe,.com,.vbs,.pif).
Vírus Stealth	**Programado para se esconder e enganar o antivírus durante uma varredura deste programa**. Tem a capacidade de se remover da memória temporariamente para evitar que antivírus o detecte.
Vírus de Script	**Propagam-se por meio de scripts**, nome que designa uma sequência de comandos previamente estabelecidos e que são executados automaticamente em um sistema, sem necessidade de intervenção do usuário. **Dois tipos de scripts muito usados** são os projetados com as linguagens Javascript (JS) e Visual Basic Script (VBS). Tanto um quanto o outro podem ser inseridos em páginas Web e interpretados por navegadores como Internet Explorer e outros. Assim como as macros, os *scripts* não são necessariamente maléficos.

Vírus de Telefone Celular	Propaga de telefone para telefone através da tecnologia bluetooth ou da tecnologia MMS (Multimedia Message Service). O serviço MMS é usado para enviar mensagens multimídia, isto é, que contêm não só texto, mas também sons e imagens, como vídeos, fotos e animações. A infecção ocorre da seguinte forma: o usuário recebe uma mensagem que diz que seu telefone está prestes a receber um arquivo e permite que o arquivo infectado seja recebido, instalado e executado em seu aparelho; o vírus, então, continua o processo de propagação para outros telefones, através de uma das tecnologias mencionadas anteriormente. Os vírus de celular diferem-se dos vírus tradicionais, pois normalmente não inserem cópias de si mesmos em outros arquivos armazenados no telefone celular, mas podem ser especificamente projetados para sobrescrever arquivos de aplicativos ou do sistema operacional instalado no aparelho.
Vírus Companheiros ou Replicadores (Spawning)	Nesse caso, o **arquivo de vírus** é contido **em um arquivo separado**, que é (geralmente) **renomeado de modo que ele seja executado em vez do programa que a vítima pensou** que estava carregando. **Possui o mesmo nome do arquivo executável, porém com outra extensão**. Ex.: sptrec.com (vírus) < sptrec.exe (executável).
Vírus de Boleto	**Altera informações dos boletos**.
Vírus Encriptado (Vírus Criptografado)	Possui **uma parte do seu código criptografado** para dificultar a detecção.

Worms (Vermes)

Programas parecidos com vírus, mas que na verdade **são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador** (observe que os worms APENAS se copiam, **não infectam outros arquivos**, eles mesmos são os arquivos). Além disso, geralmente utilizam as redes de comunicação para infectar outros computadores (via e-mails, Web, FTP, redes das empresas etc.).

Diferentemente do vírus, **o *worm* NÃO embute cópias de si mesmo em outros programas ou arquivos e NÃO necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.**

ATENÇÃO

Os **Worms** podem se espalhar de diversas maneiras, mas a propagação via rede é a mais comum. Sua característica marcante é a replicação (cópia funcional de si mesmo) e infecção de outros computadores **SEM intervenção humana** e SEM **necessidade de um programa hospedeiro**.

Worms são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias.

Esquematizando:

VÍRUS	**WORM**
É um programa (ou parte de um programa) que se anexa a um arquivo de programa qualquer.	Programa.
Propaga-se inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.	NÃO embute cópias de si mesmo em outros programas ou arquivos. Propaga-se automaticamente pelas redes, enviando copias de si mesmo de computador para computador.
Depende da execução do programa ou arquivo hospedeiro para ser ativado.	**NÃO** necessita ser explicitamente executado para se propagar. Basta que se tenha execução direta de suas cópias ou a exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Bots (“Robôs”)

De modo similar ao worm, é um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de software instalado em um computador.

Adicionalmente ao worm, dispõe de mecanismos de comunicação com o invasor, permitindo que o bot seja controlado remotamente. Os bots esperam por comandos de um hacker, podendo manipular os sistemas infectados, sem o conhecimento do usuário.

Segundo CertBr (2012), a **comunicação** entre o invasor e o computador pelo bot pode ocorrer **via canais de IRC, servidores Web, redes do tipo P2P** etc. Ao se comunicar, o invasor pode enviar instruções para que **ações maliciosas** sejam executadas, **como desferir ataques, furtar dados do computador infectado e enviar spam**.

Nesse ponto, cabe destacar um termo que já foi cobrado várias vezes em prova pela banca! Trata-se do significado de **botnet,** junção da contração das palavras **robot (bot) e network (net)**.

Obs.: **uma rede infectada por bots é denominada de botnet (também conhecida como REDE ZUMBI), sendo composta geralmente por milhares desses elementos maliciosos, que ficam residentes nas máquinas, aguardando o comando de um invasor.**

Quanto mais **zumbis** (Zombie Computers) participarem da botnet, mais potente ela será. Um invasor que tenha controle sobre uma botnet pode utilizá-la para:

- **coletar informações** de um grande número de computadores;
- **"clicar" em anúncios** e gerar receitas fraudulentas;
- **enviar spam** em grande escala;
- **hospedar sites de *phishing***;
- **iniciar ataques de negação de serviço** que impedem o uso de serviços online etc.

Obs.: **botnets** fornecem aos criminosos cibernéticos capacidade de processamento e conectividade de Internet em escala gigantesca. **É desse modo que eles são capazes de enviar milhões de *e-mails* de *spam* ou infectar milhões de PCs por hora** (SYMANTEC, 2014).

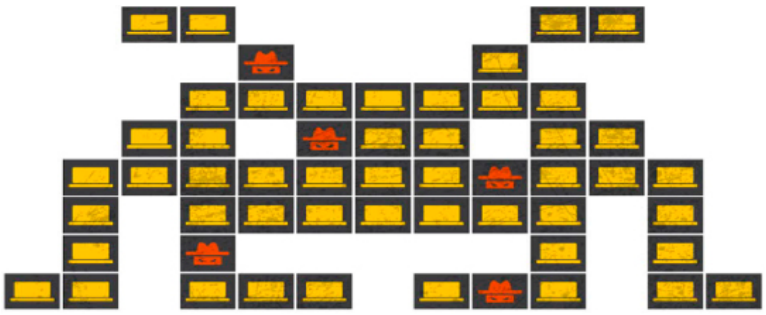


Figura. Botnet (Symantec, 2014)

O **esquema** apresentado a seguir destaca **o funcionamento básico de uma botnet** (CERT.br, 2012):

- o atacante propaga um tipo específico de bot, com a intenção de infectar e conseguir a maior quantidade possível de máquinas zumbis;
- essas máquinas zumbis ficam então à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;
- quando o controlador deseja que uma ação seja realizada, ele envia às máquinas zumbis os comandos a serem executados, usando, por exemplo, redes do tipo **P2P** ou servidores centralizados;
- as máquinas zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlador;
- quando a ação é encerrada, as **máquinas zumbis** voltam a ficar à espera dos próximos comandos a serem executados.

Trojan Horse (Cavalo de Troia)

É um programa aparentemente inofensivo que entra em seu computador na forma de cartão virtual, álbum de fotos, protetor de tela, jogo etc., **e que, quando executado (com a sua autorização), parece lhe divertir, mas, por trás abre portas de comunicação do seu computador para que ele possa ser invadido.**

Obs.: **por definição, o Cavalo de Troia distingue-se de um vírus ou de um *worm* por NÃO infectar outros arquivos, NEM propagar cópias de si mesmo automaticamente.**

Os trojans atuais são divididos em duas partes, que são: o servidor e o cliente.

- Normalmente, o **servidor** encontra-se oculto em algum outro arquivo e, no momento em que o arquivo é executado, o servidor se instala e se oculta no computador da vítima;
- Nesse momento, o computador já pode ser acessado pelo **cliente**, que enviará informações para o servidor executar certas operações no computador da vítima.

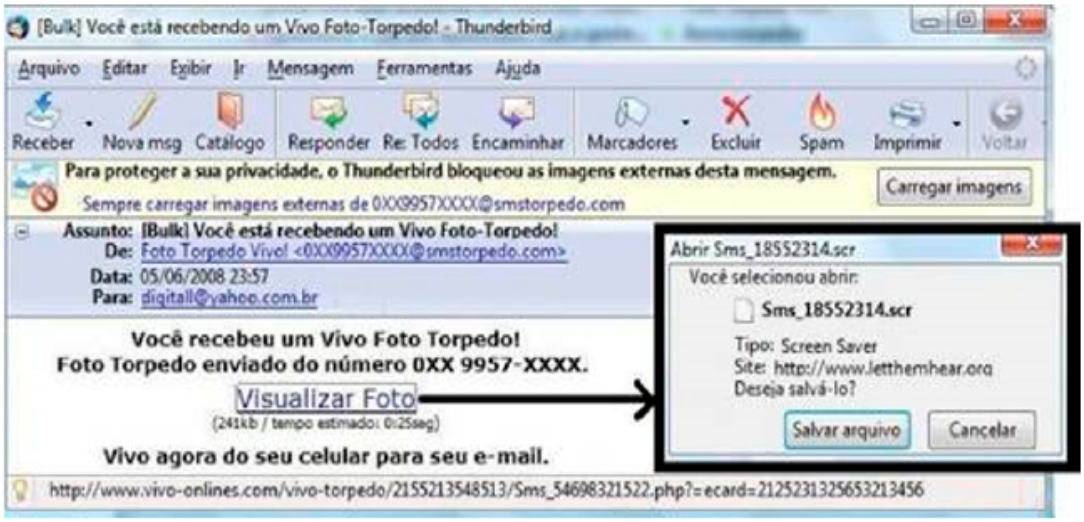


Figura. Um spam contendo um código malicioso conhecido como Cavalo de Troia. Ao passar o mouse sobre o link, veja que o site mostrado não é da Vivo. O usuário será infectado se clicar no link e executar o anexo.

Uma das características do Cavalo de Troia (Trojan Horse) é que ele facilita ação de outros ataques!

Obs.: **o cavalo de troia não é um vírus, pois não se duplica e não se dissemina como os vírus. Na maioria das vezes, ele irá instalar programas para possibilitar que um invasor tenha controle total sobre um computador.**

Estes programas podem permitir que o invasor:

- veja e copie ou destrua todos os arquivos armazenados no computador;
- faça a instalação de keyloggers ou screenloggers (descubra as senhas digitadas pelo usuário);
- realize o furto de senhas e outras informações sensíveis, como números de cartões de crédito;
- faça a inclusão de **backdoors**, para permitir que um atacante tenha total controle sobre o computador; formate o disco rígido do computador etc.

Exemplos comuns de Cavalos de Troia são programas que você recebe ou obtém de algum site e que parecem ser apenas cartões virtuais animados, álbuns de fotos de alguma celebridade, jogos, protetores de tela, entre outros. Enquanto estão sendo executados, estes programas podem ao mesmo tempo enviar dados confidenciais para outro computador, instalar *backdoors*, alterar informações, apagar arquivos ou formatar o disco rígido.

Há **diferentes tipos de trojans**, classificados de acordo com as ações maliciosas que costumam executar ao infectar um computador. Alguns desses tipos apontados por Certbr (2012) são:

- **Trojan Downloader**: instala outros códigos maliciosos, obtidos de sites na Internet;
- **Trojan Dropper**: instala outros códigos maliciosos, embutidos no próprio código do trojan;
- **Trojan Backdoor**: inclui backdoors, possibilitando o acesso remoto do atacante ao computador.

A mensagem seguinte disponibilizava ao usuário um arquivo com backdoor e trojan bancário, conforme visto no relatório com o conteúdo da análise realizada sobre o arquivo.

Trojan DoS: instala ferramentas de negação de serviço e as utiliza para desferir ataques.

Trojan Destrutivo: altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.

Trojan Clicker: redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.

Trojan Proxy: instala um servidor de proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam.

Trojan Spy: instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.

Trojan Banker: coleta dados bancários do usuário, através da instalação de programas spyware que são ativados nos acessos aos sites de Internet Banking. É similar ao Trojan Spy, porém com objetivos mais específicos.

Spyware

Trata-se de um **programa espião (spy em inglês = espião), que tem por finalidade monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.**

Obs.: segundo a norma ABNT ISO/IEC 27000, **Spyware é um software enganador que coleta informações particulares ou confidenciais de um usuário de computador.** Informações podem incluir assuntos como websites mais visitados ou informações mais sensíveis, como senhas.

Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.

Vamos à diferença entre seu uso (Cert.BR,2012):

- **Legítimo**: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado;

- **Malicioso**: quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns tipos específicos de programas spyware são:

Keylogger (Copia as Teclas Digitadas!)

É capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.

Dentre as informações capturadas podem estar o texto de um e-mail, dados digitados na declaração de Imposto de Renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito. Em muitos casos, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site específico de comércio eletrônico ou Internet Banking. Normalmente, o keylogger contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de e-mails).

Screenloggers (Copia as Telas Acessadas!)

As instituições financeiras desenvolveram os teclados virtuais para evitar que os keyloggers pudessem capturar informações sensíveis de usuários. Então, foram desenvolvidas formas mais avançadas de keyloggers, também conhecidas como **screenloggers** capazes de: **armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado**.

Normalmente, o keylogger vem como parte de um programa spyware ou cavalo de troia. Desta forma, é necessário que este programa seja executado para que o keylogger se instale em um computador.

Geralmente, tais programas vêm anexados a e-mails ou estão disponíveis em sites na Internet. Existem ainda programas leitores de e-mails que podem estar configurados para executar automaticamente arquivos anexados às mensagens. Neste caso, o simples fato de ler uma mensagem é suficiente para que qualquer arquivo anexado seja executado.

Adware (Advertising Software) (Exibe Propagandas!)

Projetado especificamente para **apresentar propagandas**.

Este tipo de programa geralmente não prejudica o computador. Cert.Br (2103) destaca que ele pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos.

Quando o seu uso é feito de forma maliciosa, pode abrir uma janela do navegador apontando para páginas de cassinos, vendas de remédios, páginas pornográficas etc. Também as propagandas apresentadas podem ser direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo realizado.

Obs.: segundo a norma ABNT ISO/IEC 27000, **adware** é um **aplicativo que joga publicidade para os usuários e/ou reúne informações sobre o comportamento online do usuário.** O aplicativo pode ou não ser instalado com o conhecimento ou consentimento do usuário, ou ser forçado para o usuário através de termos de licenciamento para outro software.

Trackware

São programas que **rastreiam a atividade do sistema**, reúnem informações do sistema ou rastreiam os hábitos do usuário, retransmitindo essas informações a organizações de terceiros.

As informações reunidas por esses programas não são confidenciais nem identificáveis. Os programas de trackware são instalados com o consentimento do usuário e também podem estar contidos em pacotes de outro software instalado pelo usuário.

Exploits

É um código criado para **explorar uma vulnerabilidade** existente em um programa. Um **exploit kit** reúne e empacota esses códigos para que sejam de uso fácil e até comercializável entre criminosos. Esses kits **são usados na web para criar páginas maliciosas que, uma vez visitadas, conseguem contaminar o computador com algum vírus.**

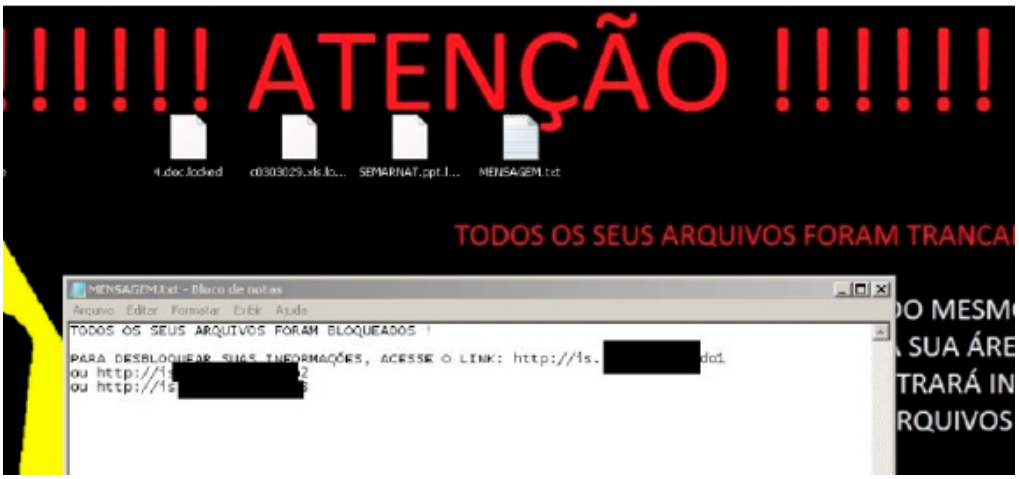
Ransomware (Pede Resgate!)

O termo vem da palavra "**resgate**" em inglês (ransom) unida ao sufixo de **malware**. Ciber-criminosos **sequestram** os dados salvos no equipamento e exigem um **resgate** para liberar o acesso a eles. Cifram esses dados usando **alta criptografia** "impossível" de ser quebrada.

Em outras palavras, **são softwares maliciosos que, ao infectarem um computador, criptografam todo ou parte do conteúdo do disco rígido.** Os responsáveis pelo software exigem da vítima, um pagamento pelo "resgate" dos dados.

O **Pagamento de resgates** é feito via **bitcoin (moeda virtual anônima), cartões pré-pagos** (Amazon, iTunes etc.), sendo que o preço do resgate pode variar. Exemplo: usuário doméstico (50 a 300 dólares), empresas (de 500 a 4000 dólares). No entanto, **o pagamento do resgate não garante que você conseguirá restabelecer o acesso!**

Chantagens: algumas versões são impossíveis de recuperar (mesmo pagando), outras deletam arquivos (com contagem regressiva).



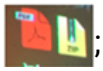
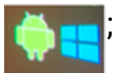
Alvo dos ransomwares: planilhas, documentos, banco de dados, arquivos de texto, imagens, programas financeiros, projetos (AutoCad), etc.

Existem dois tipos de ransomware:

- **Ransomware Locker**: impede que você acesse o equipamento infectado;
- **Ransomware Crypto**: impede que você acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia.

Além de infectar o equipamento o ransomware **também costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los** também.

Métodos de infecção por ransomware:

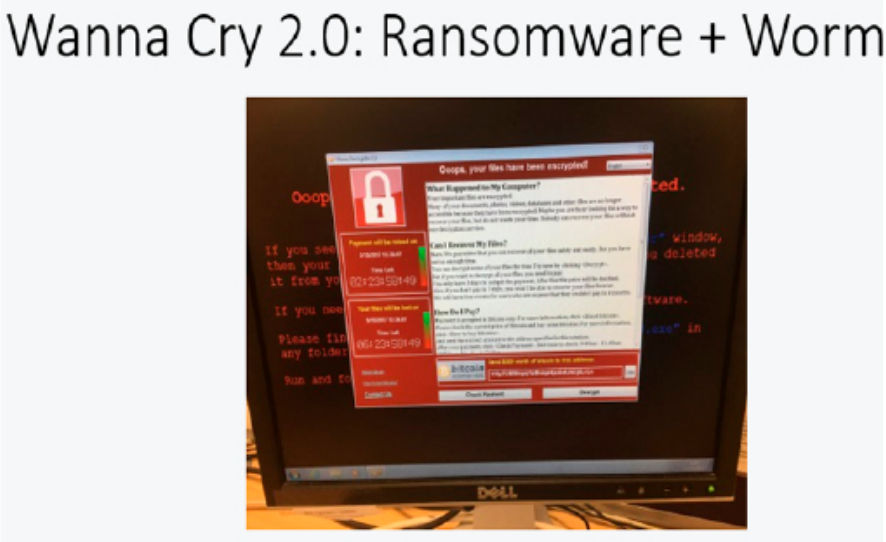
- arquivos maliciosos em e-mail (inclui PDF, DOC etc.)  ;
- explorando falhas de sistemas não atualizados  ;
- exploit kits instalados em sites infectados;
- disseminados pela rede, em unidades compartilhadas  ;
- servidores: acesso remoto (RDP, VNC etc.).

Uma nova modalidade de ransomware já está preparada **para ataques aos dispositivos móveis**, com Android, por exemplo.

Para se proteger de ransomware você deve tomar os mesmos cuidados que toma para evitar os outros códigos maliciosos, como ter um antivírus instalado e ser cuidadoso ao clicar em links ou abrir arquivos. **Fazer backups regularmente** também é essencial para proteger os

seus dados pois, se seu equipamento for infectado, a única solução realmente efetiva para acessá-los novamente é buscá-los em seus backups.

Tendência: em 2020 haverá um aumento de ataques de trojans ransomware a equipamentos conectados à internet.



Exemplo: conforme foi noticiado pela imprensa, um **ataque cibernético** de grandes proporções iniciou-se em **12/05/17**, afetando diversas empresas ao redor do mundo. A ameaça principal detectada neste cenário é um **ransomware**, conhecido pelas variantes de **WannaCry** ou HydraCrypt**, que infecta computadores utilizando o sistema operacional Microsoft Windows através de uma vulnerabilidade no serviço SMB, utilizado para o compartilhamento de arquivos via rede**.

Resumindo, **trata-se de uma infecção por malware do tipo ransomware, que se caracteriza por criptografar os arquivos dos usuários e exigir um resgate em dinheiro eletrônico,** conhecido como Bitcoin (moeda virtual), **para que seja fornecida a senha de recuperação desses dados**. Além de ransomware, atua como um **worm**, propagando-se automaticamente pelas redes com máquinas desatualizadas (uma vez que um computador seja infectado, ele tentará propagar essa infecção para os demais computadores conectados na mesma rede).

É importante reforçar algumas **medidas que o usuário deve seguir para que se proteja contra essa ameaça**:

- mantenha seu computador sempre atualizado;
- tenha sempre uma cópia de segurança (backup) dos seus arquivos;
- tenha atitudes seguras no uso dos recursos de TI.

Fique alerta e pratique as regras de segurança tanto no ambiente doméstico quanto nos ambientes externos!

Backdoors (Abre Portas!)

Normalmente, um atacante procura garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão. Na maioria dos casos, também é intenção do atacante poder retornar ao computador comprometido sem ser notado. **A esses programas que permitem o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim**, dá-se o nome de **backdoor**.

A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da Internet). Pode ser incluído por um invasor ou através de um cavalo de troia.

Programas de administração remota, como BackOrifice, NetBus, Sub-Seven, VNC e Radmin, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como backdoors.

Bomba Lógica (Logic Bomb)

Programa em que o **código malicioso é executado quando ocorre um evento predefinido** (como uma data que está se aproximando ou quando uma determinada palavra ou sequência de caracteres é digitada no teclado

pelo usuário). Uma ação de uma bomba lógica seria, por exemplo, fazer com que determinadas informações de um banco de dados sejam removidas numa determinada data.

As bombas lógicas são difíceis de detectar porque são frequentemente instaladas por quem tem autorização no sistema, seja pelo usuário devidamente autorizado ou por um administrador. **Alguns tipos de vírus são considerados bombas lógicas, uma vez que têm um circuito de disparo planejado por hora e data**.

Hijackers

São **programas ou scripts que "sequestram" navegadores de Internet**, principalmente o Internet Explorer. Quando isso ocorre, o hijacker altera a página inicial do browser e impede o usuário de mudá-la. Nesse momento, vira uma confusão só, porque muitas vezes aparecem páginas de conteúdo erótico e o usuário não consegue alterá-las!

Scareware (Software de Engano, Software de Verificação Desonesto ou Fraudware)

É um **software malicioso que faz com que os usuários de computadores acessem sites infestados por malware.**

O scareware pode vir na forma de caixas suspensas. Elas aparecem como "avisos legítimos" de empresas de software antivírus, alegando que os arquivos de seu computador foram infectados.

São tão habilmente criados que os usuários ficam assustados e pagam uma taxa para adquirir rapidamente um software que irá resolver o suposto problema. Mas o que eles acabam baixando é um falso software antivírus que na verdade é um malware destinado a roubar os dados pessoais da vítima.

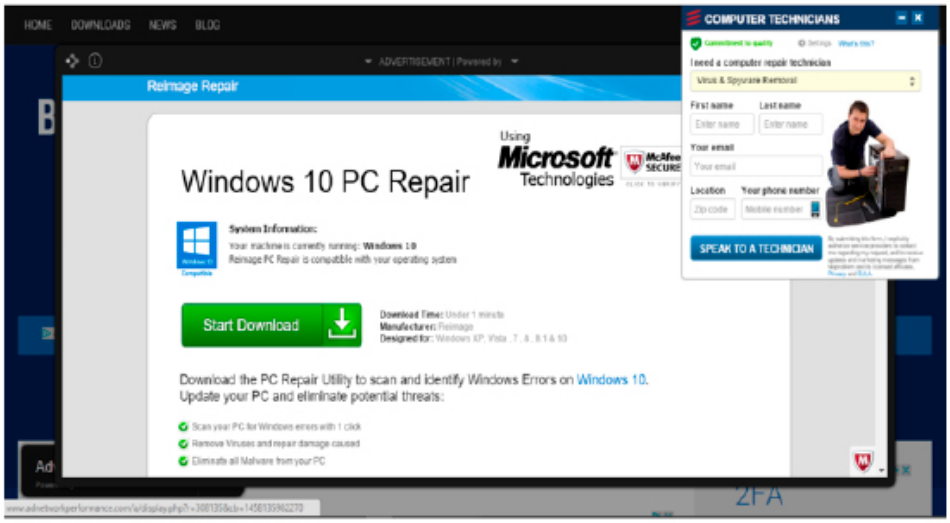


Figura. Exemplo de Mensagem Suspeita. (Fonte: https://www.windowsteam.com.br/windows-defender-vai-por-um-fim-nos-chatissimos-scarewares/, Acesso em: jan/2019).

Rootkit (Busca Alterar a Ação do Sistema Operacional!)

Tipo de malware cuja **principal intenção é se camuflar, para assegurar a sua presença no computador comprometido, impedindo que seu código seja encontrado por qualquer antivírus.** Isto é possível porque tem a capacidade de interceptar as solicitações feitas ao sistema operacional, podendo alterar o seu resultado.

O invasor, após instalar o rootkit, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

Um rootkit pode fornecer programas com as mais diversas **funcionalidades**. Dentre eles, merecem destaque:

- **programas para esconder atividades e informações** deixadas pelo invasor, tais como arquivos, diretórios, processos etc.;
- **backdoors**, para assegurar o acesso futuro do invasor ao computador comprometido;
- **programas para remoção de evidências em arquivos de logs**;
- **sniffers**, para capturar informações na rede onde o computador está localizado, como por exemplo senhas que estejam trafegando em claro, ou seja, sem qualquer método de criptografia;
- **scanners**, para mapear potenciais vulnerabilidades em outros computadores.

A tabela seguinte apresenta um comparativo interessante relacionado aos malwares:

	Vírus	Worm	Bot	Trojan	Spyware	Backdoor	Rootkit
Como é obtido:							
Recebido automaticamente pela rede		✓	✓				
Recebido por *e-mail*	✓	✓	✓	✓	✓		
Baixado de *sites* na Internet	✓	✓	✓	✓	✓		
Compartilhamento de arquivos	✓	✓	✓	✓	✓		
Uso de mídias removíveis infectadas	✓	✓	✓	✓	✓		
Redes sociais	✓	✓	✓	✓	✓		
Mensagens instantâneas	✓	✓	✓	✓	✓		
Inserido por um invasor		✓	✓	✓	✓	✓	✓
Ação de outro código malicioso		✓	✓	✓	✓	✓	✓
Como ocorre a instalação:							
Execução de um arquivo infectado	✓						
Execução explícita do código malicioso		✓	✓	✓	✓		
Via execução de outro código malicioso						✓	✓
Exploração de vulnerabilidades		✓	✓			✓	✓
Como se propaga:							
Insere cópia de si próprio em arquivos	✓						
Envia cópia de si próprio automaticamente pela rede		✓	✓				
Envia cópia de si próprio automaticamente por *e-mail*		✓	✓				
Não se propaga				✓	✓	✓	✓
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✓			✓			✓
Consome grande quantidade de recursos		✓	✓				
Furta informações sensíveis			✓	✓	✓		
Instala outros códigos maliciosos		✓	✓	✓			✓
Possibilita o retorno do invasor						✓	✓
Envia *spam* e *phishing*			✓				
Desfere ataques na Internet		✓	✓				
Procura se manter escondido	✓				✓	✓	✓

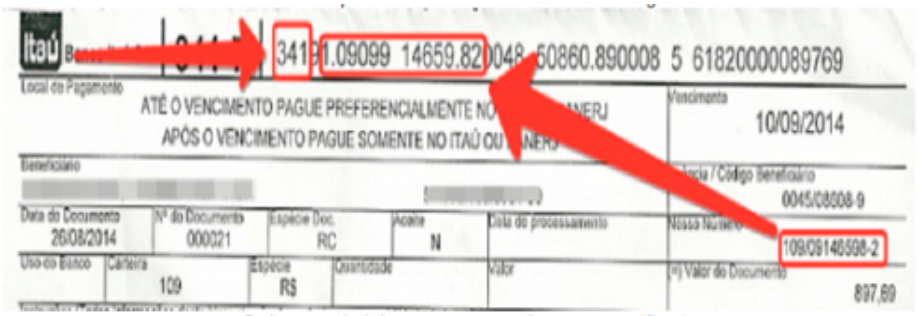
Tabela. Resumo comparativo entre códigos maliciosos (Fonte: CertBr).Disponível em: http://cartilha.cert.br/malware/

Bolware

É um **malware (geralmente vírus de boleto) que infecta computadores e realiza a falsificação de dados de boletos bancários**, realizando determinadas mudanças no documento, alterando muitas vezes a conta em que o valor será depositado, criando problemas para o usuário que - sem saber - perde o valor do pagamento realizado, como também para as empresas que iriam receber o pagamento.

Verifique em todo boleto impresso se o número do banco (3 primeiros dígitos da linha digitável) corresponde ao banco emissor do boleto. **A maioria dos vírus costuma trocar o banco, apesar de alguns poucos preservarem o banco original que emitiu o boleto.**

Confira o campo "Nosso número" no boleto, ele deve estar presente na linha digitável, caso contrário é provável que o boleto foi adulterado.



Boleto verdadeiro: campos que devem ser verificados

Boleto falso: campo "Nosso número" diferente no código de barras

Se precisar reemitir um boleto bancário ou recalculá-lo, **use o site do Banco, jamais use um site desconhecido.**

Caso o código de barras esteja ilegível na hora do pagamento, **desconfie** do boleto e **NÃO PAGUE**, busque certificar-se de que o mesmo não tenha sido alterado.

Crack

Programas utilizados para **quebrar senhas e licenças de softwares**. São encontrados facilmente na Internet, mas em sites que não são merecedores de confiança.

Sniffers (Farejadores ou ainda Capturadores de Pacotes)

Por padrão, os computadores (pertencentes à mesma rede) escutam e respondem somente pacotes endereçados a eles. Entretanto, é possível utilizar um software que coloca a interface num estado chamado de ***modo promíscuo***. Nessa condição **o computador pode monitorar e capturar os dados trafegados através da rede, não importando o seu destino legítimo**. **Os programas responsáveis por capturar os pacotes de rede são chamados *Sniffers, Farejadores ou ainda Capturadores de Pacote***. Eles exploram o fato do tráfego dos pacotes das aplicações TCP/IP não utilizar nenhum tipo de cifragem nos dados.

Dessa maneira um *sniffer* atua na rede "farejando pacotes" na tentativa de encontrar certas informações (trata-se de um malware quando fareja pacotes da rede em busca de informações **não autorizadas**), como nomes de usuários, senhas ou qualquer outra informação transmitida que não esteja criptografada.

A dificuldade no uso de um *sniffer* é que o atacante precisa instalar o programa em algum ponto estratégico da rede, como entre duas máquinas, (com o tráfego entre elas passando pela máquina com o farejador) ou em uma rede local com a interface de rede em modo promíscuo.

APT (Advanced Persistent Threat - Ameaça Persistente Avançada)

Comumente usada para se referir a ameaças cibernéticas, em particular a prática de espionagem via internet por intermédio de uma variedade de técnicas de coleta de informações que são consideradas valiosas o suficiente para que o agente espião despenda tempo e recursos para obtê-las.

Anti-bots/Anti-apts: novas ferramentas de proteção contra ameaças desse tipo!

Criptojacking é um tipo de ataque que consiste no roubo do processamento de computadores para minerar criptomoedas ilegalmente.

7. Hoaxes (Boatos)

São as **histórias falsas recebidas por e-mail, sites de relacionamentos, Whatsapp e na Internet em geral**, cujo conteúdo, além das conhecidas correntes, consiste em apelos dramáticos de cunho sentimental ou religioso, supostas campanhas filantrópicas, humanitárias ou de socorro pessoal ou, ainda, falsos vírus que ameaçam destruir, contaminar ou formatar o disco rígido do computador.

Figura. Exemplos de hoax (boato)

A figura seguinte destaca um exemplo de hoax recebido em minha caixa de e-mails. O remetente e destinatários foram embaçados de propósito por questão de sigilo.

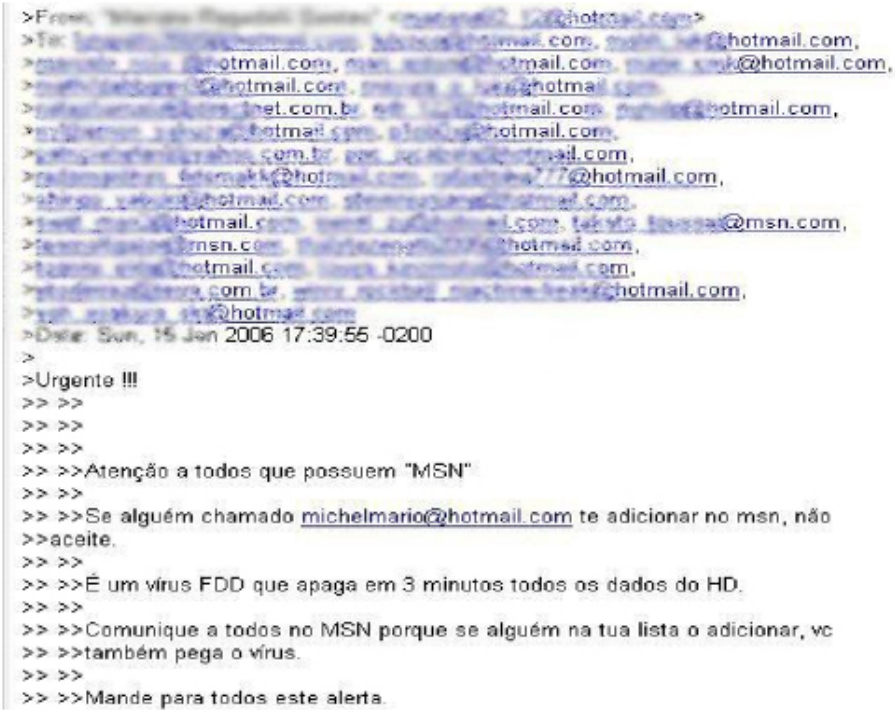

>From: [redacted]
>To: [redacted]
>Date: Sun, 15 Jan 2006 17:39:56 -0200
>
>Urgente !!!
>> >>
>> >>
>> >>
>> >>Atenção a todos que possuem "MSN"
>> >>
>> >>Se alguém chamado michelmario@hotmail.com te adicionar no msn, não
>>aceite.
>> >>
>> >>É um vírus FDD que apaga em 3 minutos todos os dados do HD.
>> >>
>> >>Comunique a todos no MSN porque se alguém na tua lista o adicionar, vc
>> >>também pega o vírus.
>> >>
>> >>Mande para todos este alerta.

Figura. Exemplo de um hoax (boato) bastante comum na Internet

Outros casos podem ser visualizados na Internet, vide por exemplo os endereços listados a seguir para que você se certifique e não repasse mensagens desse tipo:

- http://www.quatrocantos.com/LENDAS/.
- http://www.boatos.org

8. Principais Golpes Aplicados via Internet

A seguir, apresentamos alguns dos **principais golpes aplicados na Internet:**

Phishing (Phishing Scam, ou apenas Scam)

É um tipo de fraude eletrônica projetada para roubar informações particulares que sejam valiosas para cometer um roubo ou fraude posteriormente.

O golpe de phishing é realizado por uma pessoa mal-intencionada através da criação de um website falso e/ou do envio de uma mensagem eletrônica falsa, geralmente um e-mail ou recado através de scrapbooks como existia no Orkut, entre outros exemplos.

Utilizando de pretextos falsos, tenta enganar o receptor da mensagem e induzi-lo a fornecer informações sensíveis (números de cartões de crédito, senhas, dados de contas bancárias etc.).

Obs.: **a palavra phishing (de fishing) vem de uma analogia criada pelos fraudadores, em que "iscas" (e-mails) são usadas para "pescar" informações sensíveis (senhas e dados financeiros, por exemplo) de usuários da Internet.**

Atualmente, este termo vem sendo utilizado também para se referir aos seguintes casos:

- **páginas falsas de comércio eletrônico ou Internet Banking;**
- **páginas falsas de redes sociais** ou de companhias aéreas;
- **mensagem que, no próprio conteúdo, apresenta formulários** para o preenchimento e envio de dados pessoais e financeiros de usuários;
- **mensagens contendo links para instalação de códigos maliciosos,** projetados para furtar dados pessoais e financeiros. Ao clicar nesse link aparecerá uma mensagem de erro ou uma janela pedindo que você salve o arquivo. Após ter sido salvo, quando você for abri-lo/executá-lo, será instalado um código malicioso no computador do usuário;
- **solicitação de recadastramento** em que o usuário recebe uma mensagem, supostamente enviada pelo grupo de suporte da instituição de ensino que frequenta ou da empresa em que trabalha, informando que o serviço de e-mail está passando por manutenção e que é necessário o recadastramento. Para isto, é preciso que você forneça seus dados pessoais, como nome de usuário e senha.

As duas figuras seguintes apresentam "iscas" (e-mails) utilizadas em golpes de phishing, uma envolvendo o Banco de Brasil e a outra o Serasa.

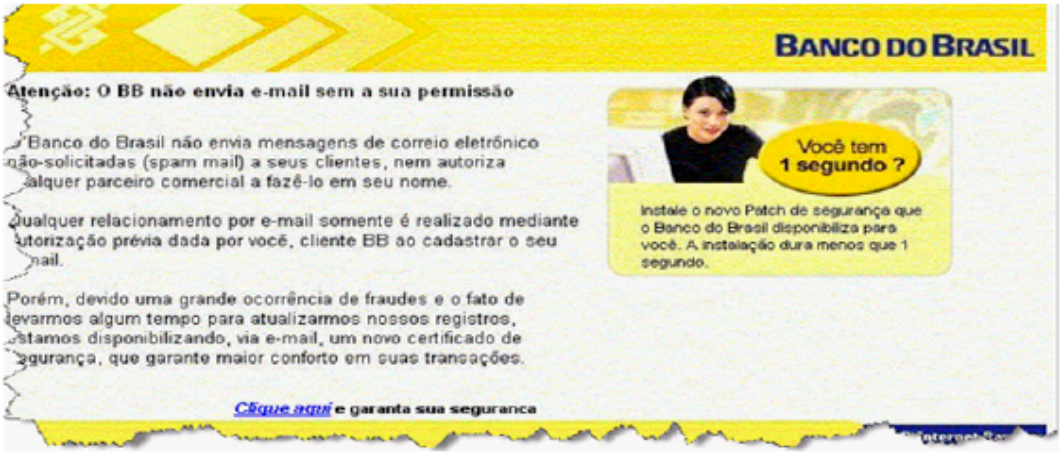


Figura. Isca de Phishing Relacionada ao Banco do Brasil

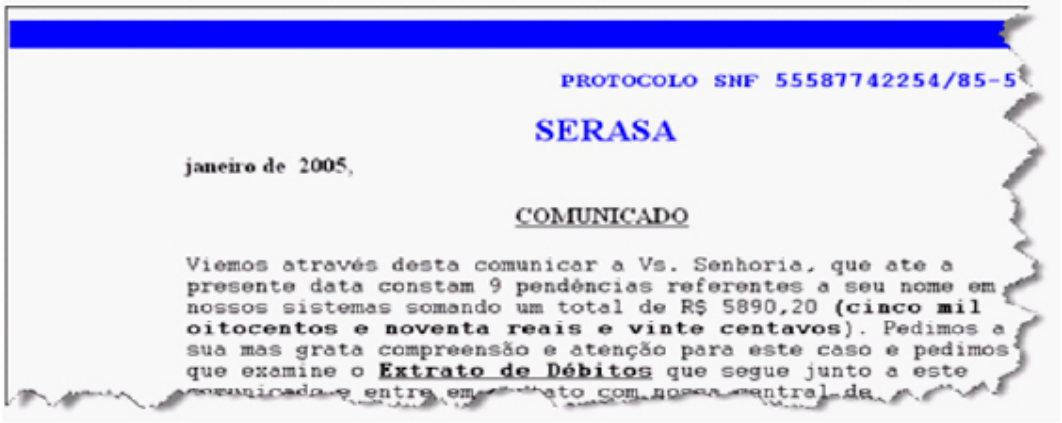


Figura. Isca de Phishing Relacionada ao SERASA

Spear Phishing

É um **golpe de e-mail direcionado com o objetivo único de obter acesso não autorizado aos dados sigilosos.**

Diferente dos golpes de phishing, que realizam ataques amplos e dispersos, o **spear phishing foca em um grupo ou organização específicos**. A intenção é roubar propriedade intelectual, dados financeiros, segredos comerciais ou militares e outros dados confidenciais.

Ele funciona da seguinte maneira: um e-mail é recebido, aparentemente de uma fonte confiável, no entanto ele leva o destinatário a um site falso cheio de malware. Esses e-mails costumam usar táticas inteligentes para chamar a atenção das vítimas. Por exemplo, o FBI

alertou sobre golpes de spear phishing, nos quais os e-mails pareciam ser do National Center for Missing and Exploited Children.

Veja mais: http://securityintelligence.com/fbi-warns-increase-spear-phishingattacks/#.VHzBpfnF_h4.

Obs.: **o ataque de spear phishing, que é uma tentativa de fraude por falsificação de e-mail, tem como alvo uma organização específica e objetiva, normalmente, conseguir acesso não autorizado a dados sigilosos** (CESPE/2014/ANATEL).

Pharming

É uma **técnica que utiliza o sequestro ou a "contaminação" do servidor DNS (Domain Name Server) para levar os usuários a um site falso, alterando o DNS do site de destino.** O sistema também pode redirecionar os usuários para sites autênticos através de *proxies* controlados, que podem ser usados para monitorar e interceptar a digitação.

Os sites falsificados coletam números de cartões de crédito, nomes de contas, senhas e números de documentos. Isso é feito através da exibição de um pop-up para roubar a informação antes de levar o usuário ao site real. O programa mal-intencionado usa um certificado autoassinado para fingir a autenticação e induzir o usuário a acreditar nele o bastante para inserir seus dados pessoais no site falsificado. Outra forma de enganar o usuário é sobrepor a barra de endereço e status de navegador para induzi-lo a pensar que está no site legítimo e inserir suas informações.

Nesse contexto, **programas criminosos podem ser instalados nos PCs dos consumidores para roubar diretamente as suas informações**. Na maioria dos casos, o usuário não sabe que está infectado, percebendo apenas uma ligeira redução na velocidade do computador ou falhas de funcionamento atribuídas a vulnerabilidades normais de software.

Golpe de Sextorsão

E-mails em que os criminosos alegam possuir um vídeo da vítima, que foi **gravado enquanto ela estaria assistindo a um site pornô.**

Novo golpe usa sites pornô e senhas hackeadas para chantagear usuários

Golpe usa senhas vazadas há anos para tornar ameaças mais verídicas e extorquir vítima

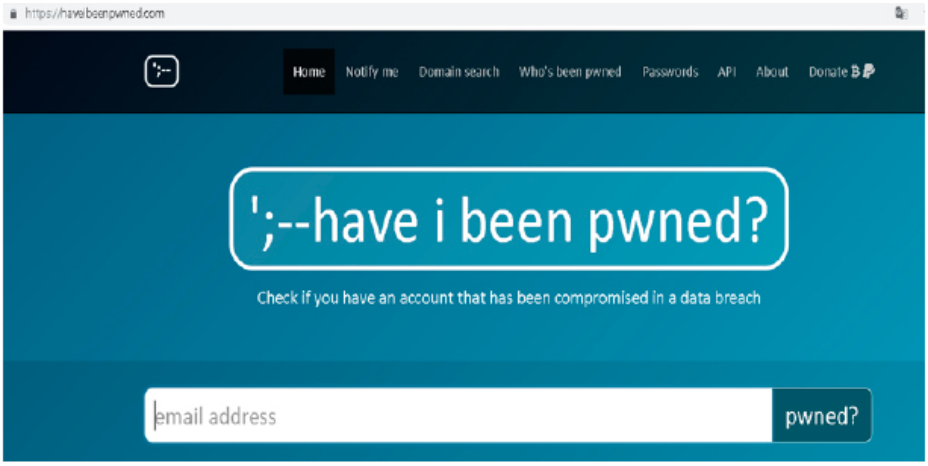
Por Raquel Freire, para o TechTudo

12/07/2018

A mensagem é mentirosa, mas inclui uma senha hackeada **real** do usuário, o que aumenta sua veracidade. O propósito é chantagear a vítima, coagida a pagar por exemplo US$ 1.400 (cerca de R$ 5.380, em conversão direta) em **Bitcoins**.

A mensagem ameaça divulgar o suposto vídeo para todos os contatos do **Facebook**, **Messenger** e da própria conta de e-mail caso o depósito em criptomoedas não seja realizado dentro de 24 horas.

No site listado a seguir, é possível **checar se o seu e-mail foi comprometido** em algum momento. Não será surpresa se ele estiver por lá listado! Cuidado, então, para que você não seja a próxima vítima do golpe de extorsão.



9. Ataques na Internet

Ataque, segundo a norma ISO/IEC 27000 (2009) **é a tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado, ou fazer uso não autorizado de um ativo.**

Os ataques costumam ocorrer na Internet com diversas motivações (financeiras, ideológicas, comerciais etc.), tendo-se em vista diferentes alvos e usando variadas técnicas. "Qualquer

serviço, computador ou rede que seja acessível via Internet pode ser alvo de um ataque, assim como qualquer computador com acesso à Internet pode participar de um ataque" (CertBr,2012).

A seguir, destacamos algumas das técnicas utilizadas nos ataques, que podem ser cobradas na sua prova.

Interceptação de Tráfego (Sniffing)

Processo de **captura das informações da rede** por meio de um **software de escuta de rede** (**sniffer**, farejador ou ainda capturador de pacote), capaz de interpretar as informações transmitidas no meio físico.

Segundo o CertBr (2012), essa técnica pode ser utilizada de forma:

- **Legítima:** por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados;
- **Maliciosa:** por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

Note que "as informações capturadas por esta técnica são armazenadas na forma como trafegam, ou seja, informações que trafegam criptografadas apenas serão úteis ao atacante se ele conseguir decodificá-las" (CertBr,2012).

Denial of Service (DoS)

Os **ataques de negação de serviço** (**denial of service - DoS**) consistem em impedir o funcionamento de uma máquina ou de um serviço específico. No caso de ataques a redes, geralmente ocorre que os usuários legítimos de uma rede não consigam mais acessar seus recursos.

O DoS acontece quando um atacante envia vários pacotes ou requisições de serviço de uma vez, com objetivo de sobrecarregar um servidor e, como consequência, impedir o fornecimento de um serviço para os demais usuários, causando prejuízos.

Obs.: **no DoS o atacante utiliza um computador para tirar de operação um serviço ou computador(es) conectado(s) à Internet!**

Cabe ressaltar que se uma rede ou computador sofrer um **DoS**, isto não significa que houve uma invasão, pois o objetivo de tais ataques é indisponibilizar o uso de um ou mais computadores, e não invadi-los.

ATENÇÃO

Um dos mais conhecidos **ataques** a um computador conectado a uma rede é o de **negação de serviço** (**DoS – *Denial Of Service***), que ocorre quando um determinado recurso torna-se indisponível devido à ação de um agente que tem por finalidade, em muitos casos, diminuir a capacidade de processamento ou de armazenagem de dados.

Distributed Denial of Service (DDoS) -> São os Ataques Coordenados!

Para isso, o atacante faz o uso de uma **botnet** (**rede de computadores zumbis sob comando do atacante**) para bombardear o servidor com requisições, fazendo com que o ataque seja feito de forma distribuída (Distributed Denial of Service – DDoS).

Obs.: **no DDoS - ataque de negação de serviço distribuído-, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.**

Ataque de Força Bruta (Brute Force)

Força bruta consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário (Certbr,2012).

Esse é um método muito poderoso para descoberta de senhas, no entanto é extremamente lento porque cada combinação consecutiva de caracteres é comparada. Ex: aaa, aab, aac..... aaA, aaB, aaC... aa0, aa1, aa2, aa3. aba, aca, ada...

Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta. Dispositivos móveis, que estejam protegidos por senha, além de poderem ser atacados pela rede, também podem ser alvo deste tipo de ataque caso o atacante tenha acesso físico a eles (Certbr,2012).

Se um atacante tiver conhecimento do seu nome de usuário e da sua senha ele pode efetuar ações maliciosas em seu nome como, por exemplo (Certbr,2012):

- trocar a sua senha, dificultando que você acesse novamente o site ou computador invadido;
- invadir o serviço de e-mail que você utiliza e ter acesso ao conteúdo das suas mensagens e à sua lista de contatos, além de poder enviar mensagens em seu nome;
- acessar a sua rede social e enviar mensagens aos seus seguidores contendo códigos maliciosos ou alterar as suas opções de privacidade;
- invadir o seu computador e, de acordo com as permissões do seu usuário, executar ações, como apagar arquivos, obter informações confidenciais e instalar códigos maliciosos.

Mesmo que o atacante não consiga descobrir a sua senha, você pode ter problemas ao acessar a sua conta caso ela tenha sofrido um ataque de força bruta, pois muitos sistemas bloqueiam as contas quando várias tentativas de acesso sem sucesso são realizadas (Certbr, 2012).

Apesar dos **ataques de força bruta** poderem ser realizados manualmente, na grande maioria dos casos, eles são realizados com o uso de ferramentas automatizadas facilmente obtidas na Internet e que permitem tornar o ataque bem mais efetivo (Certbr, 2012).

As tentativas de adivinhação costumam ser baseadas em (Certbr, 2012):

- **dicionários de diferentes idiomas** e que podem ser facilmente obtidos na Internet;
- **listas de palavras comumente usadas**, como personagens de filmes e nomes de times de futebol;
- **substituições óbvias de caracteres**, como trocar “a” por “@” e “o” por “0”’;
- **sequências numéricas e de teclado**, como “123456”, “qwert” e “1qaz2wsx”;
- **informações pessoais**, de conhecimento prévio do atacante ou coletadas na Internet em redes sociais e blogs, como nome, sobrenome, datas e números de documentos.

Um ataque de força bruta, dependendo de como é realizado, pode resultar em um ataque de negação de serviço, devido à sobrecarga produzida pela grande quantidade de tentativas realizadas em um pequeno período de tempo (Certbr,2012).

Pichação ou Desfiguração de Página (Defacement)

É uma técnica que consiste **em alterar o conteúdo da página Web de um site**. Dentre as vulnerabilidades (falhas de segurança) que podem ser exploradas nesse tipo de ataque, podemos citar: erros da aplicação Web ou no servidor de aplicação Web etc.

Spoofing

É uma prática em que **um computador envia comandos a outro se fazendo passar por um terceiro.**

Varredura em Redes, ou Scan

Permite **efetuar buscas minuciosas em redes**, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

10. Spams

São mensagens de correio eletrônico não autorizadas ou não solicitadas, sendo um dos grandes responsáveis pela propagação de códigos maliciosos, disseminação de golpes e venda ilegal de produtos.

O spam não é propriamente uma ameaça à segurança, mas é um **portador comum delas**. São spams, por exemplo, os e-mails falsos que recebemos como sendo de órgãos como Receita Federal ou Tribunal Superior Eleitoral. Nesse caso, os spams costumam induzir o usuário a instalar um dos malwares que vimos anteriormente.

11. Cookies

São pequenos arquivos que são instalados em seu computador durante a navegação, permitindo que os sites (servidores) obtenham determinadas informações. É isto que permite que alguns sites o cumprimentem pelo nome, saibam quantas vezes você o visitou etc.

A seguir destacamos alguns dos **riscos relacionados ao uso de cookies** (CERTBR, 2013):

- **informações coletadas pelos cookies** podem ser indevidamente compartilhadas com outros sites e afetar a sua privacidade;
- **exploração de vulnerabilidades existentes no computador.** Ao acessar uma página da Web o seu navegador disponibiliza uma série de informações sobre a máquina como hardware, sistema operacional e programas instalados. Os cookies podem ser utilizados para manter referências contendo estas informações e usá-las para explorar possíveis vulnerabilidades existentes em seu computador;
- **autenticação automática**: quando utilizamos as opções como “Lembre-se de mim” e “continuar conectado” nos sites visitados, os cookies guardam essas informações para autenticações futuras. Em caso de uma máquina contaminada, essa prática pode permitir que outras pessoas se autentiquem como você;
- **coleta de informações pessoais**: dados preenchidos em formulários Web também podem ser gravados em cookies, coletados por atacantes ou códigos maliciosos e indevidamente acessados, caso não estejam criptografados;

- **coleta de hábitos de navegação**: quando você acessa diferentes sites onde são usados cookies de terceiros, pertencentes a uma mesma empresa de publicidade, é possível a esta empresa determinar seus hábitos de navegação e, assim, comprometer a sua privacidade.

Prevenção

Segundo o CertBr (2013), **não é indicado bloquear totalmente o recebimento de cookies,** pois isto pode impedir o uso adequado ou até mesmo o acesso a determinados sites e serviços. Para se prevenir dos riscos, mas sem comprometer a sua navegação, há algumas dicas que você deve seguir, como:

- ao usar um navegador Web baseado em níveis de permissão, como o Internet Explorer, procure não selecionar níveis de permissão inferiores a "médio";
- em outros navegadores ou programas leitores de e-mail, configure para que, por padrão, os sites não possam definir cookies e crie listas de exceções, cadastrando sites considerados confiáveis e onde o uso de cookies é realmente necessário, como Webmails e de Internet Banking e comércio eletrônico;
- caso você, mesmo ciente dos riscos, decida permitir que por padrão os sites possam definir cookies, procure criar uma lista de exceções e nela cadastre os sites que deseja bloquear;
- configure para que os cookies sejam apagados assim que o navegador for fechado;
- configure para não aceitar cookies de terceiros (ao fazer isto, a sua navegação não deverá ser prejudicada, pois apenas conteúdos relacionados a publicidade serão bloqueados);
- utilize opções de navegar anonimamente, quando usar computadores de terceiros (ao fazer isto, informações sobre a sua navegação, incluindo cookies, não serão gravadas).

Veja que, quando você altera uma configuração de privacidade ela é aplicada aos novos cookies, mas não aos que já estão gravados em seu computador. Assim, ao fazer isto, **é importante que você remova os cookies já gravados para garantir que a nova configuração seja aplicada a todos.**

12. Compartilhamento de Recursos

Ao fazer um compartilhamento de recursos do seu computador, como diretórios, discos, e impressoras, com outros usuários, **pode estar permitindo**:

- o acesso não autorizado a recursos ou informações sensíveis;
- **que seus recursos sejam usados por atacantes,** caso não sejam definidas senhas para controle de acesso ou sejam usadas senhas facilmente descobertas.

Procedimentos de Segurança

Diante desse grande risco, uma série de procedimentos, considerados como "**boas práticas de segurança**" podem ser implementados para salvaguardar os **ativos** (que é o que a segurança da informação busca proteger) da organização (CertBR, 2006).

Adotar Estratégias para Redução de Spams

Como podemos reduzir o volume de spam que chega até nossas caixas postais?

A resposta é bem simples! Basta **navegar de forma consciente na rede**. Este conselho é o mesmo que recebemos para zelar pela nossa segurança no trânsito ou ao entrar e sair de nossas casas.

A seguir destacamos as principais dicas que foram reportadas pelo CertBr (2012) para que os usuários da Internet desfrutem dos recursos e benefícios da rede, com segurança:

- **Preservar as informações pessoais,** tais como: endereços de e-mail, dados pessoais e, principalmente, cadastrais de bancos, cartões de crédito e senhas. **Um bom exercício é pensar que ninguém forneceria seus dados pessoais a um estranho na rua, ok? Então, por que liberá-la na Internet?**
- **Ter, sempre que possível, e-mails separados para assuntos pessoais, profissionais, para as compras e cadastros online.** Certos usuários mantêm um e-mail somente para assinatura de listas de discussão.

Obs.: no caso das promoções da Internet, geralmente, será necessário preencher formulários. **Ter um e-mail para cadastros online é uma boa prática para os usuários com o**

> **perfil descrito.** Ao preencher o cadastro, procure desabilitar as opções de recebimento de material de divulgação do site e de seus parceiros, pois justamente nesse item é que muitos usuários atraem spam, inadvertidamente!

- Não ser um "clicador compulsivo", ou seja, o usuário deve procurar controlar a curiosidade de verificar sempre a indicação de um site em um e-mail suspeito de spam. **Pensar, analisar as características do e-mail e verificar se não é mesmo um golpe ou código malicioso**;
- Não ser um "caça-brindes", "papa-liquidações" ou "destruidor-de-promoções", rs! Ao receber e-mails sobre brindes, promoções ou descontos, reserve um tempo para analisar o e-mail, sua procedência e verificar no site da empresa as informações sobre a promoção em questão. Vale lembrar que os sites das empresas e instituições financeiras têm mantido alertas em destaque sobre os golpes envolvendo seus serviços. Assim, a visita ao site da empresa pode confirmar a promoção ou alertá-lo sobre o golpe que acabou de receber por e-mail!
- **Ferramentas de combate ao spam** (**antispams**) são geralmente disponibilizadas do lado dos servidores de e-mail, filtrando as mensagens que são direcionadas à nossa caixa postal. Importante que se tenha um filtro antispam instalado, ou ainda, usar os recursos antispam oferecidos por seu provedor de acesso.
- Além do antispam, existem outras ferramentas bastante importantes para o usuário da rede: antispyware, firewall pessoal, antivírus etc.

Cuidados com Contas e Senhas

Uma senha pode ser descoberta ao ser usada em computadores infectados; ao ser usada em sites falsos; por meio de tentativas de adivinhação; ao ser capturada enquanto trafega na rede, sem estar criptografada; por meio do acesso ao arquivo onde a senha foi armazenada caso ela não tenha sido gravada de forma criptografada; com o uso de técnicas de engenharia social, como forma a persuadi-lo a entregá-la voluntariamente; pela observação da movimentação dos seus dedos no teclado ou dos cliques do mouse em teclados virtuais (CERT.BR,2012).

Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante.

Alguns elementos que você **não deve** usar na elaboração de suas senhas são: **qualquer tipo de dado pessoal** (jamais utilizar como senha seu nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você etc.)**; sequências de teclado; palavras que façam parte de listas**.

Alguns elementos que você deve usar na elaboração de suas senhas são: números aleatórios; grande quantidade de caracteres; diferentes tipos de caracteres (CERT.BR,2013).

Mais dicas:

- crie uma senha que contenha pelo menos oito caracteres, compostos de letras, números e símbolos;
- utilize uma senha diferente para cada serviço (por exemplo, uma senha para o banco, outra para acesso à rede corporativa da sua empresa, outra para acesso a seu provedor de Internet etc.);
- altere a senha com frequência;
- crie tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador;
- utilize o usuário Administrator (ou root) somente quando for estritamente necessário.

Cuidados com Malware

O **combate a códigos maliciosos** poderá envolver uma série de ações, como:

- instalação de ferramentas antivírus e antispyware no computador, lembrando de mantê-las atualizadas frequentemente. A banca pode citar ferramentas antimalware nesse contexto também;
- não realizar abertura de arquivos suspeitos recebidos por e-mail;
- fazer a instalação de patches de segurança e atualizações corretivas de softwares e do sistema operacional quando forem disponibilizadas (proteção contra worms e bots) etc.

Vírus

Instale e mantenha atualizado um bom programa antivírus.

Atualize as assinaturas do antivírus, de preferência diariamente.

Configure o antivírus para verificar os arquivos obtidos pela Internet, discos rígidos (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e pen drives.

Desabilite no seu programa leitor de e-mails a autoexecução de arquivos anexados às mensagens.

Não execute ou abra arquivos recebidos por e-mail ou por outras fontes, mesmo que venham de pessoas conhecidas. Caso seja necessário abrir o arquivo, certifique-se que ele foi verificado pelo programa antivírus

Utilize na elaboração de documentos formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF ou PostScript etc.

Worms, Bots e Botnets

Siga todas as recomendações para prevenção contra vírus listadas no item anterior.

Mantenha o sistema operacional e demais softwares sempre atualizados.

Aplique todas as correções de segurança (patches) disponibilizadas pelos fabricantes, para corrigir eventuais vulnerabilidades existentes nos softwares utilizados.

Instale um firewall pessoal, que **em alguns casos** pode evitar que uma vulnerabilidade existente seja explorada **(observe que o firewall não corrige as vulnerabilidades!)** ou que um worm ou bot se propague.

Cavalos de Troia, Backdoors, Keyloggers e Spywares

Siga todas as recomendações para prevenção contra vírus, worms e bots.

Instale um firewall pessoal, que **em alguns casos** pode evitar o acesso a um backdoor já instalado em seu computador etc.

Utilize pelo menos uma ferramenta antispyware e mantê-la sempre atualizada.

Elaboração de uma Política de Segurança

É de fundamental importância a elaboração de uma Política de Segurança com o objetivo de solucionar ou minimizar as vulnerabilidades encontradas na organização

Nesse contexto, destacamos os principais itens necessários para uma boa política de segurança:

- possuir instalações físicas adequadas que ofereçam o mínimo necessário para garantia da integridade dos dados;
- controle de umidade, temperatura e pressão;
- sistema de aterramento projetado para suportar as descargas elétricas, extintores de incêndio adequados para equipamentos elétricos/eletrônicos;
- uso adequado de equipamentos de proteção e segurança tais como: UPS (“no-break”), filtro de linha, estabilizador de tensão;
- manutenção do computador, limpeza e política da boa utilização;
- utilização de sistemas operacionais que controlem o acesso de usuários e que possuem um nível de segurança bem elaborado, juntamente com o controle de senhas;
- utilização de sistemas de proteção de uma rede de computadores, tais como **Firewall** (sistema que filtra e monitora as ações na rede);
- software antivírus atualizado constantemente;
- sistema de criptografia (ferramenta que garante a segurança em todo ambiente computacional que precise de sigilo em relação às informações que manipula). No envio de mensagens uma mensagem é criptografada e se for interceptada dificilmente poderá ser lida, somente o destinatário possuir o código necessário;
- **treinamento** e conscientização de funcionários para diminuir as falhas humanas;
- realização de **backups** (cópia de segurança **para salvaguardar os dados, geralmente mantida em CDs, DVDs, fitas magnéticas, pen-drives etc., para que possam ser restaurados em caso de perda dos dados originais**).

Backup (Cópia de Segurança)

O procedimento de **backup (cópia de segurança)** pode ser descrito de forma simplificada como copiar dados de um dispositivo para o outro com o objetivo de posteriormente recuperar as informações, caso haja algum problema.

Obs.: **backup ou cópia de segurança** é uma cópia de informações importantes que está guardada em um local seguro. Objetivo: recuperação de dados em caso de falha (perda dos dados originais); acesso a versões anteriores das informações.

Um **backup** envolve cópia de dados em um meio fisicamente separado do original, regularmente, de forma a protegê-los de qualquer eventualidade.

Para a realização de um **backup**, podemos utilizar: pen-drive, CD, DVD, Blu-ray, HD externo, pastas compartilhadas na rede, armazenamento na nuvem ou cloud storage (uso do OneDrive - antigo SkyDrive, Dropbox, ou outro ambiente), Fitas-Dat etc.

Seja ele qual for a sua escolha, todos têm a mesma finalidade. **A diferença está na capacidade, vida útil e segurança de cada um**. **Não** é aconselhável o uso de outra partição do HD principal ou HD Interno, pois se acontecer algum problema com a máquina, todos os dados (originais e backup) serão perdidos.

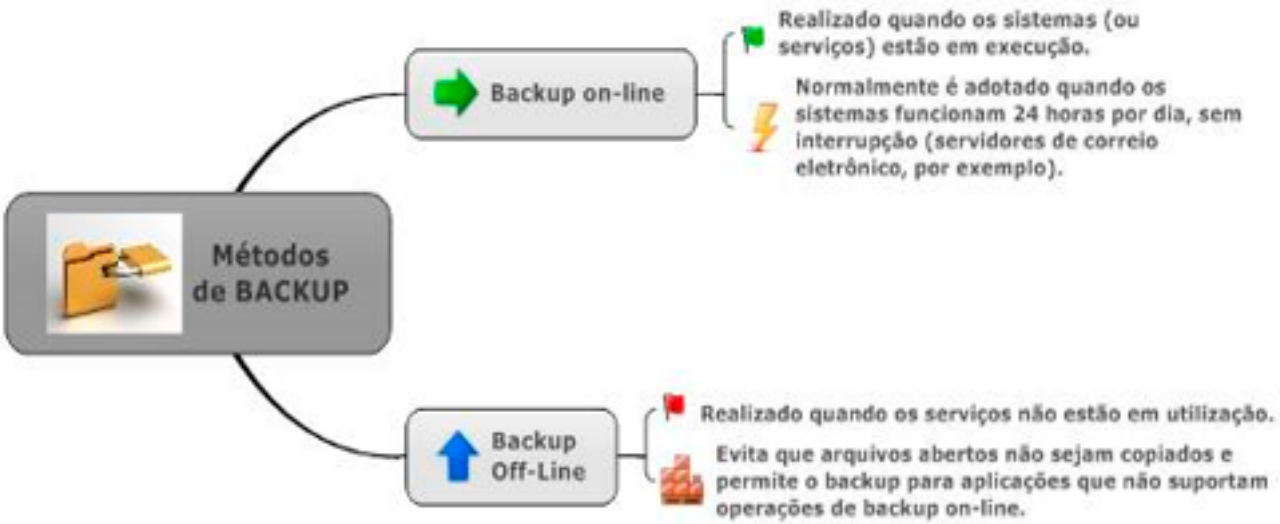
Assim, copiar nossas fotos digitais, armazenadas no HD (disco rígido), para um DVD é fazer **backup**. Se houver algum problema com o HD ou se acidentalmente apagarmos as fotos, podemos então restaurar os arquivos a partir do DVD. Nesse exemplo, chamamos as cópias das fotos no DVD de cópias de segurança ou backup.

Bem, pessoal, é importante destacar também que a proteção das informações é fundamental para o funcionamento cotidiano de qualquer empresa. Na era digital, a **informação** é um dos ativos mais valiosos, e **ter uma estratégia de backup e recuperação eficiente e gerenciável tornou-se vital para o negócio.**

Restore	**Processo de recuperação dos dados a partir de um backup**. Permite restaurar versões de arquivos de backup que tenham sido perdidas, danificadas ou alteradas acidentalmente. Você também pode restaurar arquivos individuais, grupos de arquivos ou todos os arquivos incluídos no backup.
Imagem	**Cópia de todos os dados de um dispositivo de armazenamento** (CD, DVD, HD).
Arquivamento	**Mover dados que não são mais usados** (dados históricos) para outro lugar, mas que ainda podem ser acessados em caso de necessidade.
Backup Off Site	Abrange a **replicação de dados de backup em um local geograficamente separado** do local dos sistemas de produção, além de fazer backup pela rede remota (WAN). Motivações para o backup off-site incluem recuperação de desastres, consolidação de operações de backup e economia.

13. Métodos de Backup

Existem, basicamente, **dois métodos de Backup.**



14. Atributos de Arquivos

- São informações associadas a **arquivos** e **pastas**.
- Definem o comportamento do **sistema de arquivos**.
- Podem ser acessados através das propriedades (**Alt+Enter** ou clique com botão direito do mouse no ícone do arquivo ou pasta pelo Windows).

Ao clicar com o botão direito do mouse no ícone de um arquivo do Windows, e selecionar a opção **Propriedades**; em seguida, guia **Geral** -> **Avançados**, será exibida uma caixa "**o arquivo está pronto para ser arquivado**", marcada como padrão (No **Windows XP**, leia-se **arquivo morto**).

Em uma pasta irá aparecer a caixa "**Pasta pronta para arquivamento**", conforme ilustrado nas figuras seguintes.

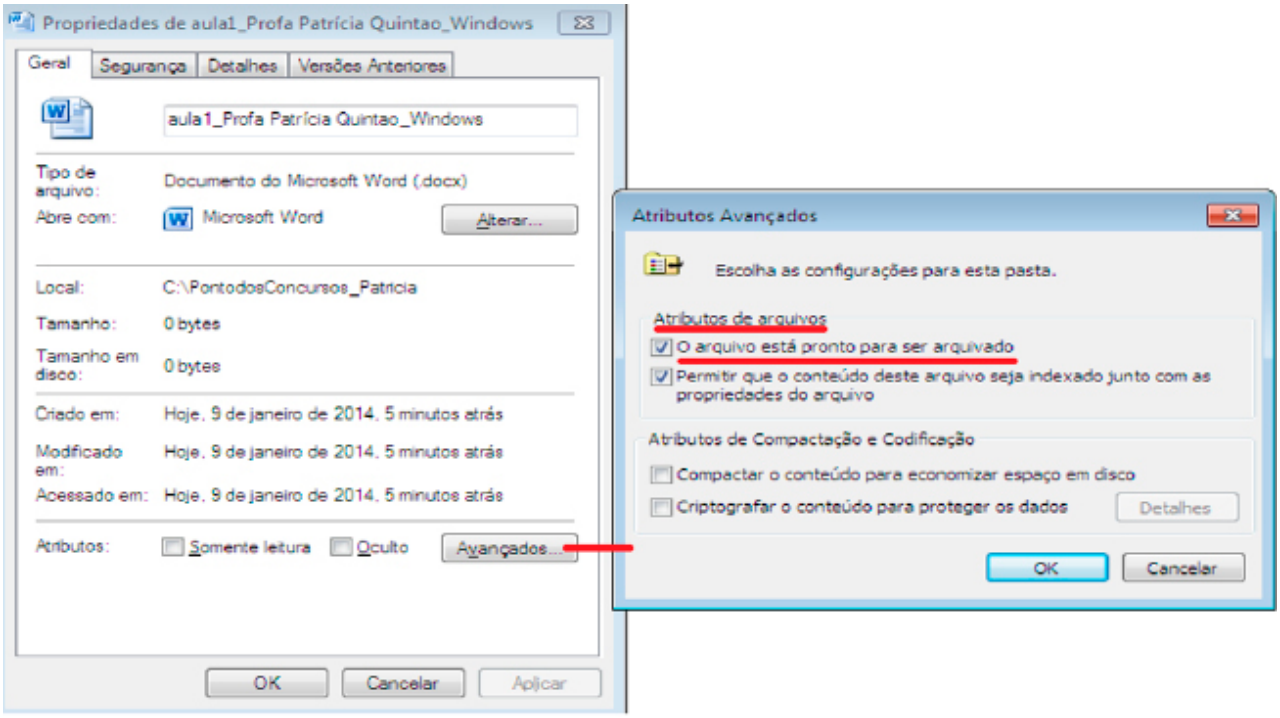


Figura. Atributos de arquivos, no Windows 7

Figura. Windows XP

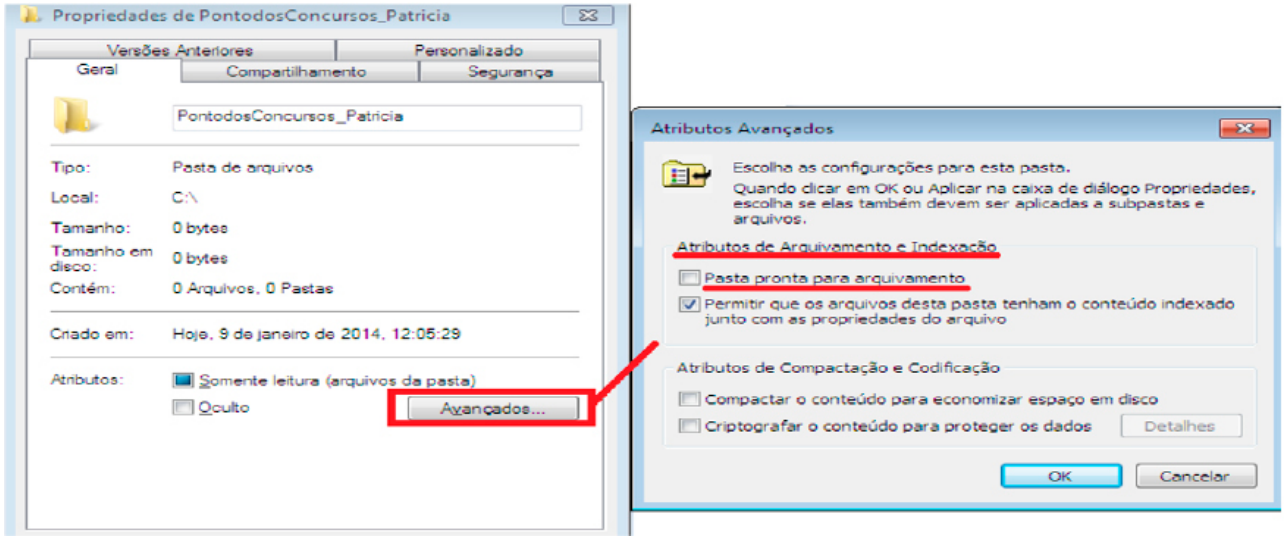
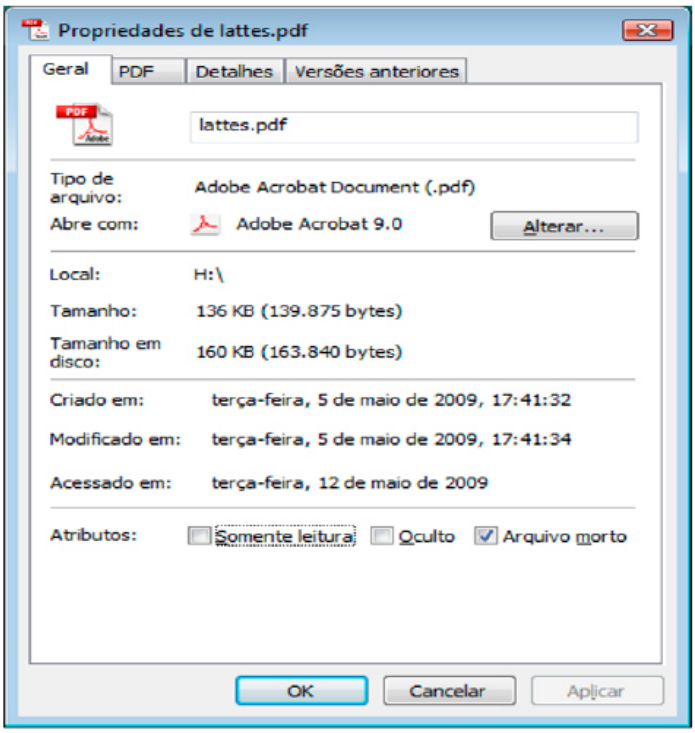


Figura. Atributos de uma pasta no Windows 7

A tela seguinte destaca opção de **"arquivo morto"** obtida ao clicar com o botão direito do mouse no arquivo intitulado lattes.pdf, do meu computador que possui o sistema operacional Windows Vista.



Assim temos:

- **Quando um arquivo/pasta está com o atributo marcado, significa que ele deverá ser copiado no próximo backup;**
- **Se estiver desmarcado, significa que, provavelmente, já foi feito um backup deste arquivo.**

15. Técnicas (Tipos) de Backup

As principais **técnicas (tipos) de Backup**, que podem ser combinadas com os mecanismos de backup online e offline, estão listadas a seguir:

NorMal (Total ou Global)	**COPIA TODOS os arquivos e pastas selecionados.** **DESMARCA o atributo de arquivamento (arquivo morto): limpa os marcadores.** **Caso necessite restaurar o backup normal, você só precisa da cópia mais recente.** **Normalmente, este backup é executado quando se cria um conjunto de backup pela 1ª vez.** **Agiliza o processo de restauração, pois somente um backup será restaurado.**

IncreMental	**Copia somente os arquivos CRIADOS ou ALTERADOS desde o último backup normal ou incremental.** O atributo de arquivamento (**arquivo morto**) **É DESMARCADO**: limpa os marcadores. **Resumindo**: **A estratégia do backup INCREMENTAL é:** **-mais rápida para fazer o backup, pois copia poucos arquivos por dia;** **-mais demorada para fazer a restauração, pois é necessário restaurar diversas fitas.**
Diferencial	Copia somente os arquivos **CRIADOS** ou **ALTERADOS desde o último backup normal ou incremental**. O atributo de arquivamento (arquivo morto) **NÃO É ALTERADO**: não limpa os marcadores.
Diferencial	**Note que o backup diferencial é acumulativo, ou seja, em cada fita de backup sempre estarão inclusos os arquivos que foram modificados desde o último backup full (normal).** **Resumindo**: **A estratégia do backup DIFERENCIAL é:** **-mais demorada para fazer o backup, pois copia cada arquivo que foi alterado do último backup normal realizado;** **-mais rápida para fazer a restauração, pois é necessário restaurar somente dois dias de backup (o normal e o do dia anterior ao crash).**
Cópia (Auxiliar ou Secundária)	Faz o backup de arquivos e pastas selecionados. O atributo de arquivamento (arquivo morto) **NÃO É ALTERADO**: não limpa os marcadores!
Diário	Copia todos os arquivos e pastas selecionados que foram **ALTERADOS DURANTE O DIA** da execução do backup. O atributo de arquivamento (arquivo morto) **NÃO É ALTERADO:** não limpa os marcadores!

16. Recuperação do Backup (Restauração de Arquivos e Pastas)

Quanto à **RECUPERAÇÃO** do backup:

- Para recuperar um backup normal, será necessária a cópia mais recente do arquivo ou da fita de backup para restaurar todos os arquivos. Geralmente, o backup normal é executado quando você cria um conjunto de backup pela primeira vez;
- Se você estiver executando **uma combinação dos backups normal e diferencial**, a restauração de arquivos e pastas exigirá o último backup normal e o último backup diferencial, já que este contém tudo que é diferente do primeiro;

- Se você utilizar **uma combinação dos backups normal e incremental**, precisará do último conjunto de backup normal e de todos os conjuntos de backups incrementais para restaurar os dados;
- O backup dos dados que utiliza **uma combinação de backups normal e incremental** exige **menos espaço** de armazenamento e é o método **mais rápido**. No entanto, a recuperação de arquivos pode ser difícil e lenta porque o conjunto de backup pode estar armazenado em vários discos ou fitas;
- O backup dos dados que utiliza **uma combinação dos backups normal e diferencial** é **mais longo**, principalmente se os dados forem alterados com frequência, mas **facilita a restauração de dados**, porque o conjunto de backup geralmente é armazenado apenas em alguns discos ou fitas.

17. Plano de Segurança para a Política de Backup

É importante estabelecer uma **política de backup** que obedeça a critérios bem definidos sobre a segurança da informação envolvida, levando-se em consideração os **serviços** que estarão disponíveis; **quem** pode acessar (perfis de usuários) as **informações**; como realizar o acesso (acesso remoto, local, senhas etc.); o que fazer em caso de falha; quais os mecanismos de segurança (antivírus), dentre outros.

Em suma, o objetivo principal dos backups é garantir a **disponibilidade** da informação. Por isso a política de backup é um processo relevante no contexto de segurança dos dados.

Autenticação

Conforme destaca Stallings (2008), "o serviço de **autenticação** refere-se à **garantia de que uma comunicação é autêntica**.

No caso de uma única mensagem, como uma advertência ou um sinal de alarme, a função do serviço de autenticação é **garantir ao destinatário que a mensagem é proveniente de onde ela afirma ter vindo**.

No caso de uma interação de saída, como a conexão de um terminal com um hospedeiro, dois aspectos estão envolvidos. **Primeiro, no momento do início da conexão, o serviço garante que**

as duas entidades são autênticas, ou seja, que cada uma é a entidade que afirma ser. **Segundo, o serviço precisa garantir que a conexão não sofra interferência de modo que um terceiro possa fingir ser uma das duas partes legítimas,** para fins de transmissão ou recepção não autorizada".

IDENTIFICAÇÃO: é a capacidade de extrair informações de um usuário ou aplicação as quais o identifiquem unicamente.

AUTENTICAÇÃO: **é a capacidade de garantir que um usuário, sistema ou informação é mesmo quem alega ser.** A autenticação é essencial para a segurança dos sistemas, ao validar a identificação dos usuários, concedendo-lhes a **AUTORIZAÇÃO** para o acesso aos recursos.

A **autenticação**, em regra, **depende** de um ou mais **modos ou fatores de autenticação**, listados a seguir:

Algo que o usuário TEM	São utilizados objetos específicos como cartões de identificação, smart cards, tokens USB.
Algo que o usuário CONHECE	São utilizadas senhas fixas, one-time passwords, sistemas de desafio-resposta.
Algo que o usuário É	Geralmente são usados meios biométricos, como impressão digital, padrão retinal, padrão de voz, reconhecimento de assinatura, reconhecimento facial.

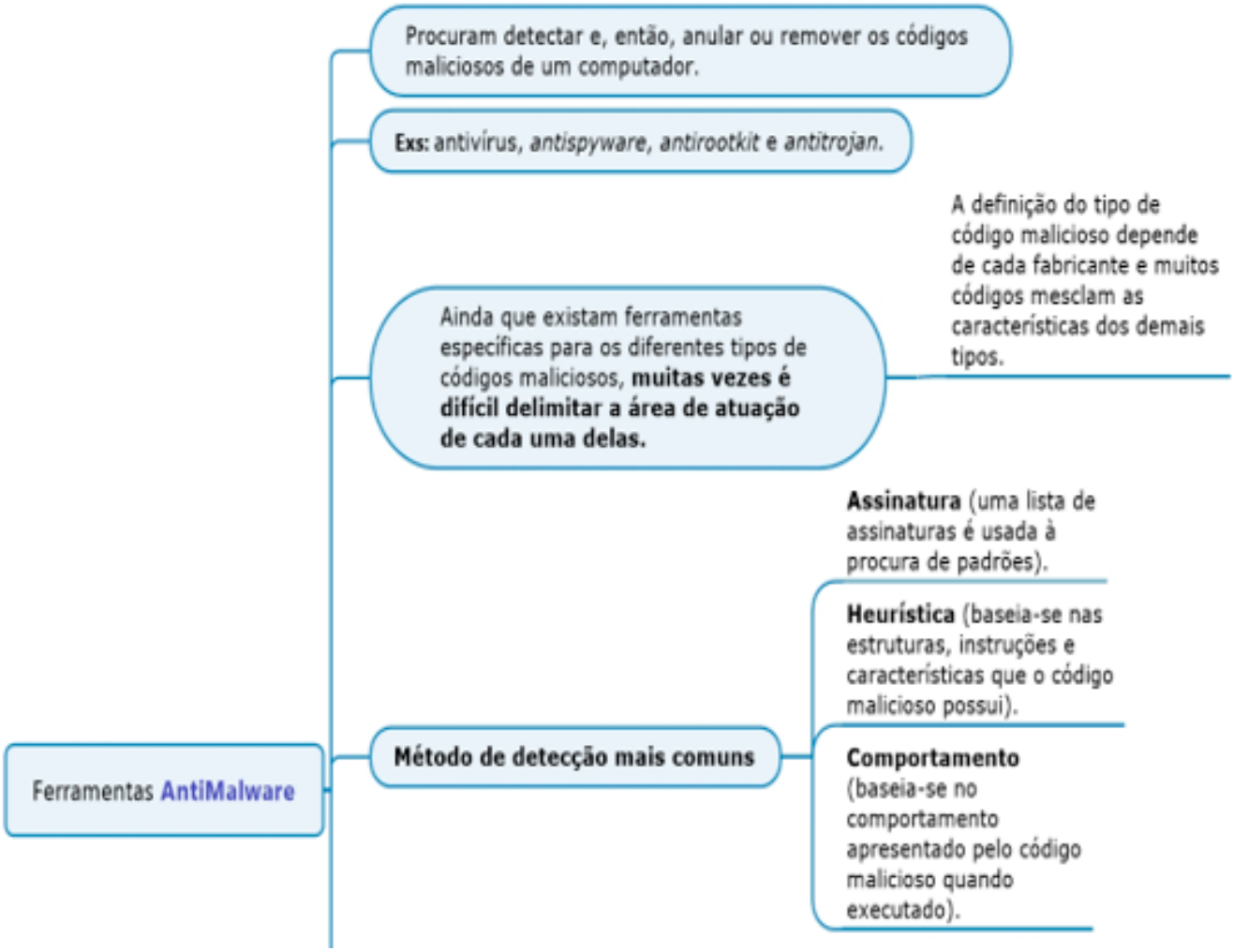
ONDE o usuário ESTÁ	Quando o acesso a sistemas só pode ser realizado em uma máquina específica, cujo acesso é restrito.

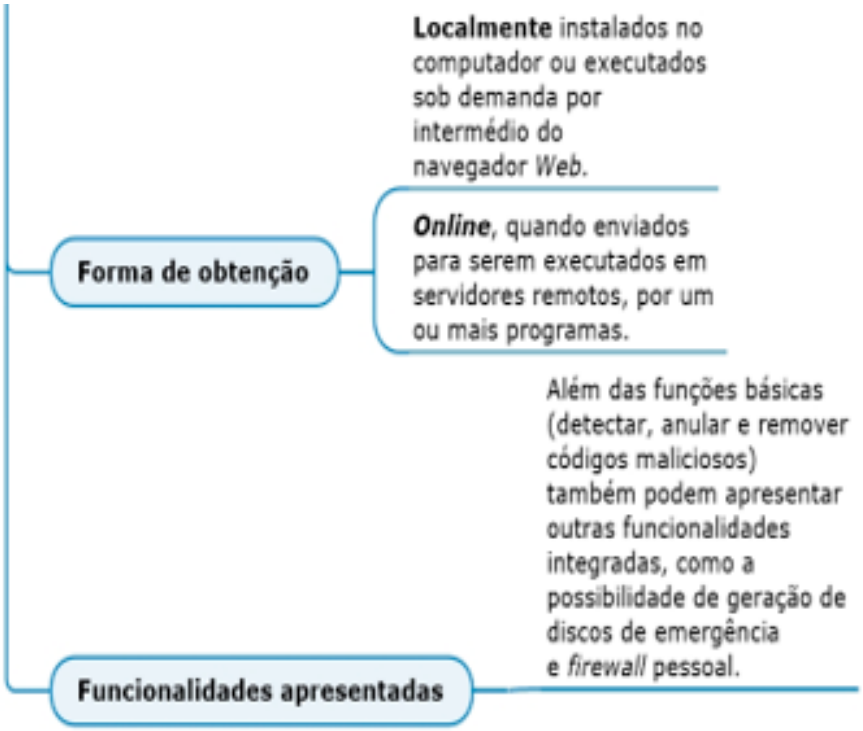
Autenticação forte consiste na autenticação por mais de um modo, ou seja, da **combinação de mais de uma maneira de autenticação**. Um exemplo disso são as transações de saque num caixa rápido. Em regra, se utiliza:

- algo que você **TEM**: um cartão da conta bancária; e
- algo que você **SABE**: a senha do cartão.

18. Aplicativos e Mecanismos de Segurança

Ferramentas Antimalware





Exemplo de antimalware online: VirusTotal - Free Online Virus, Malware and URL Scanner **https://www.virustotal.com/**

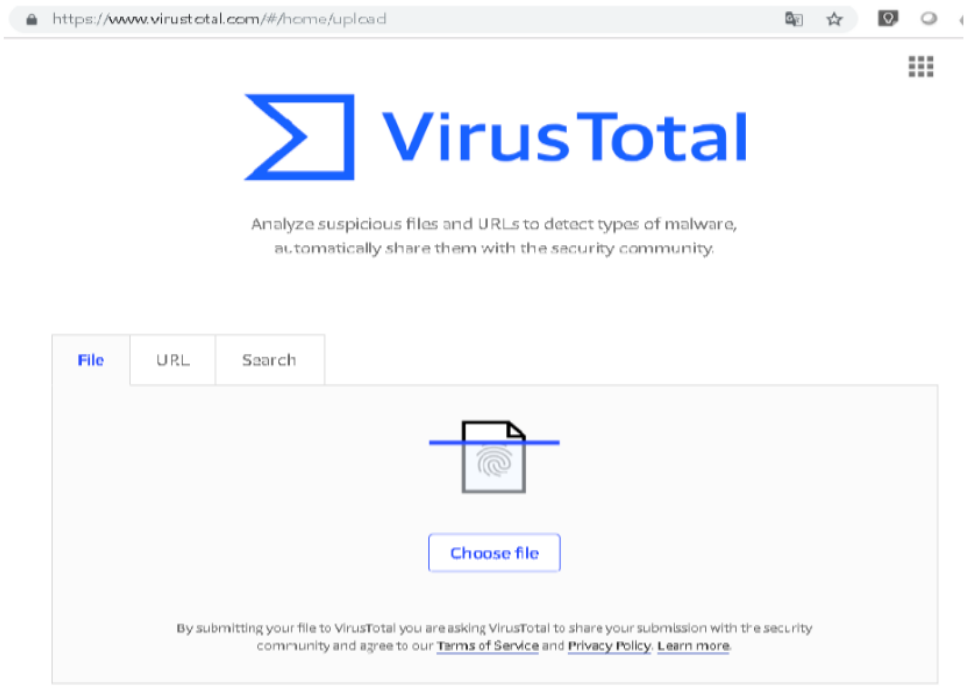


Figura. VirusTotal

Não há relação entre o custo e a eficiência de um programa, pois há versões gratuitas que apresentam mais funcionalidades que versões pagas de outros fabricantes (CertBr, 2013).

Cuidados a serem tomados, conforme destaca CertBR (2013):

- **tenha um antimalware instalado no computador** (programas online, apesar de bastante úteis, exigem que o computador esteja conectado à Internet para que funcionem corretamente e podem conter funcionalidades reduzidas);
- **utilize programas online quando suspeitar que o antimalware local esteja desabilitado/ comprometido** ou quando quiser confirmar o estado de um arquivo que já foi verificado pelo antimalware local;
- **configure o antimalware para verificar toda e qualquer extensão de arquivo**, bem como os arquivos anexados aos e-mails e aqueles obtidos pela Internet;
- configure o antimalware para **verificar automaticamente os discos rígidos e as unidades removíveis** (como pen-drives, CDs, DVDs e discos externos);
- mantenha o antimalware e o **arquivo de assinaturas** sempre atualizado;
- **evite executar simultaneamente diferentes programas antimalware** (pois podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro);
- **crie um disco de emergência e o utilize-o quando desconfiar que o antimalware instalado está desabilitado/ comprometido** ou que o comportamento do computador está estranho (mais lento, gravando ou lendo o disco rígido com muita frequência etc.).

Antivírus

Ferramentas preventivas e corretivas, que detectam (e, em muitos casos, removem) vírus de computador e outros programas maliciosos (como spywares e cavalos de troia).

Não impedem que um atacante explore alguma vulnerabilidade existente no computador. Também não evita o acesso não autorizado a um backdoor instalado no computador.

Entre as diferentes ferramentas antimalware existentes, a que engloba a maior quantidade de funcionalidades é o **antivírus**. Apesar de inicialmente eles terem sido criados para atuar especificamente sobre vírus, com o passar do tempo, passaram também a englobar as funcionalidades dos demais programas, fazendo com que alguns deles caíssem em desuso (CertBr,2013).

Os aplicativos de antivírus com escaneamento de segunda geração utilizam **técnicas heurísticas** para identificar códigos maliciosos.

Alguns autores já citam as tecnologias de detecção que usam **assinaturas e comportamento** posterior ao ataque para proteger os computadores como "envelhecidas". Já se fala em **NGAV (Next-Generation Antivírus)** que redefine o que o antivírus (AV) pode e deve fazer pela sua organização, alavancando **inteligência artificial, ciência algorítmica e aprendizado de máquina (machine learning)** para detectar e impedir a execução do malware em seus endpoints em tempo real. Ex.:Cylance.

O **programa antivírus** verifica se existem vírus conhecidos ou desconhecidos no computador.

- o vírus conhecido é aquele que pode ser detectado e identificado pelo nome;
- o vírus desconhecido é o que ainda não foi definido pelo programa antivírus.

O programa antivírus monitora continuamente o computador a fim de protegê-lo contra ambos os tipos de vírus. Para isso, quanto ao **método de detecção**, os antivírus geralmente utilizam:

- **Assinatura**: uma lista de assinaturas é usada à procura de padrões;
- **Heurística**: baseia-se nas estruturas, instruções e características que o código malicioso possui; e
- **Comportamento**: baseia-se no comportamento apresentado pelo código malicioso quando executado.

Todos esses recursos podem ser empregados nas verificações agendadas e manuais, além de serem usados pelo **Auto-Protect** para monitorar constantemente um computador. O Auto-Protect do programa Antivírus é carregado na memória durante a inicialização do Sistema Operacional, fornecendo proteção constante enquanto se trabalha. Usando o Auto-Protect, o programa antivírus automaticamente:

- elimina quaisquer *worms*, Cavalos de Troia e vírus, inclusive os de macro, e repara arquivos danificados;
- verifica a existência de vírus cada vez que se utiliza programas, discos flexíveis ou outras mídias removíveis em um computador ou utiliza documentos criados ou recebidos;

- monitora o computador em busca de sintomas atípicos que possam indicar a existência de um vírus em ação;
- protege o computador contra vírus provenientes da Internet.

É interessante manter, em seu computador:

- um antivírus funcionando constantemente (preventivamente);
- esse programa antivírus verificando os e-mails constantemente (preventivo);
- o recurso de atualizações automáticas das definições de vírus habilitado;
- as definições de vírus atualizadas constantemente (nem que para isso seja necessário, todos os dias, executar a atualização manualmente).

Principais aplicativos comerciais para antivírus:

AVG. Exemplos de edições:

- AVG Antivírus FREE, AVG Internet Security Ilimitado, AVG Ultimate.
- AVG Antivírus Business Edition, AVG Internet Security etc.

Figura. Interface do AVG para Android

Microsoft Security Essencials:

- Versão do **sistema antivírus da Microsoft;**
- Fornece proteção em tempo real ao computador, protegendo-o contra vírus, spywares e outros softwares mal-intencionados;

- Requisitos mínimos de sistema: Windows Vista (Service Pack 1 ou Service Pack 2); Windows 7 original:
  - Para Windows Vista e Windows 7, um computador com velocidade de clock de CPU de 1.0 GHz ou superior e 1 GB de RAM ou superior;
  - Vídeo VGA de 800 × 600 ou superior;
  - 200 MB de espaço disponível no disco rígido;
  - É necessária uma conexão com a Internet para a instalação e o download das definições mais recentes de vírus e spyware do Microsoft Security Essentials;
- Antes de instalar o Microsoft Security Essentials, a Microsoft destaca que é recomendável desinstalar outros softwares antivírus que estejam em execução no computador;

Obs.: **executar mais de um programa antivírus ao mesmo tempo pode causar conflitos e afetar o desempenho do computador.**

- Faz **remediação automática de malwares:** capaz de limpar automaticamente infecções altamente impactantes sem que seja necessário nenhum tipo de ação do usuário;
- A questão do **desempenho** ganhou alguns recursos extras que permitem ao usuário rodar o Microsoft Security Essentials sem que isso implique lentidão do sistema;
- **Funções básicas**: permite a **criação de pontos de restauração, scan rápido ou completo e com possibilidade de agendamento**, **proteção em tempo real e escaneamento de dispositivos removíveis conectados ao computador.**

AVAST

Exemplos de edições:

- Avast! Free Antivírus etc.

Avira

Exemplos de edições:

- Avira Free Antivírus,
- Avira Antivírus Security etc.

Panda

Exemplos de edições:

- Panda Cloud Antivírus,
- Panda Free Antivírus etc.

Figura. Panda Cloud Antivírus => Usa a "nuvem de Internet" como recurso para proteger o computador do usuário.

Bitdefender

Exemplo: Bitdefender Antivírus etc.

Kaspersky

Exemplo de edições:

- Kaspersky Anti-Virus,
- Kaspersky Security for Android etc.

Outros

A lista de aplicativos comerciais não se esgota aqui. Outras opções: TrendMicro Antivírus, F-Secure Antivírus, McAfee Antivírus etc.

Antispyware

O malware do tipo spyware pode se instalar no computador sem o seu conhecimento e a qualquer momento que você se conectar à Internet, e pode infectar o computador quando instalamos

alguns programas usando um CD, DVD ou outra mídia removível. Um spyware também pode ser programado para ser executado em horários inesperados, não apenas quando é instalado.

A ferramenta **antispyware** é uma forte aliada do antivírus, permitindo a localização e bloqueio de spywares conhecidos e desconhecidos. Exemplo de ferramentas antispyware: Windows Defender, Spybot etc.

Obs.: **nem toda ferramenta antispyware é necessariamente antivírus e vice-versa**. Há programas que apresentam as duas funções, mas isso nem sempre acontece!

Firewall

A RFC 2828 (Request for Coments n. 2828) define o termo **firewall** como sendo uma ligação entre redes de computadores que restringe o tráfego de comunicação de dados entre a parte da rede que está "dentro" ou "antes" do firewall, protegendo-a assim das ameaças da rede de computadores que está "fora" ou depois do firewall. Esse mecanismo de proteção geralmente é utilizado para proteger uma rede menor (como os computadores de uma empresa) de uma rede maior (como a Internet).

Um firewall deve ser instalado no ponto de conexão entre as redes, onde, através de regras de segurança, controla o tráfego que flui para dentro e para fora da rede protegida.

Pode ser:

- apenas um **software** sendo executado no ponto de conexão entre as redes de computadores (ex.: firewall do Windows, Iptables no Linux etc.); ou
- um **conjunto de hardware e software** (esse cenário é o mais comum de se encontrar!). O Cisco ASA é um exemplo de um firewall de hardware, que possui um software internamente para aplicação das regras de segurança que serão aplicadas a esse dispositivo.

Obs.: **vide entendimento recente da banca na prova (CESPE/PF/Perito/2019):** um **firewall** é uma **combinação de hardware e software** que isola da Internet a rede interna de uma organização, permitindo o gerenciamento do fluxo de tráfego e dos recursos da rede e o controle, pelo administrador de rede, do acesso ao mundo externo.

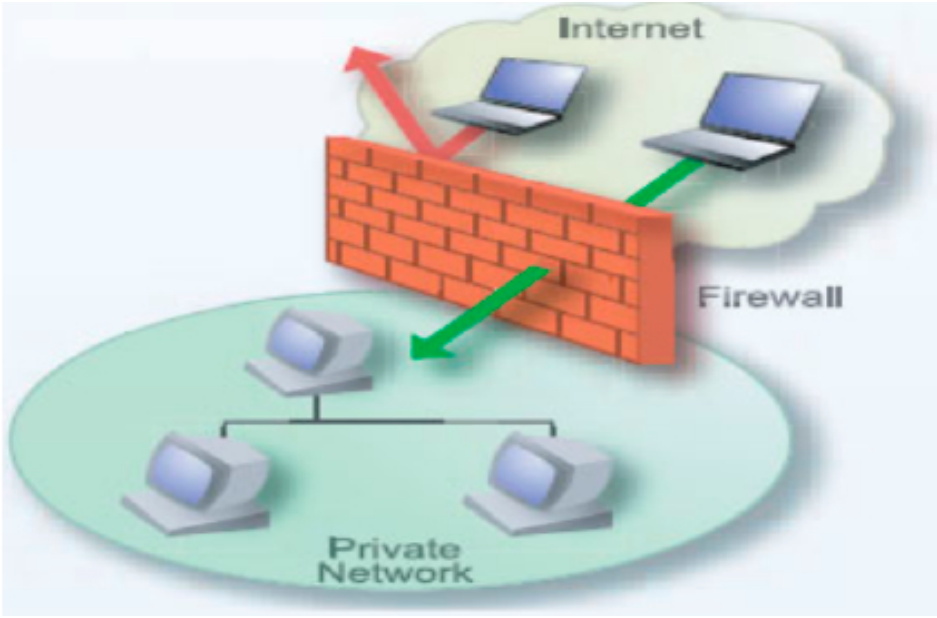


Figura. Firewall

Deve-se observar que isso o torna um potencial gargalo para o tráfego de dados e, caso não seja dimensionado corretamente, poderá causar atrasos e diminuir a performance da rede.

Os firewalls são implementados, em regra, em dispositivos que fazem a separação da rede interna e externa, chamados de **estações guardiãs** (**bastion hosts**). Quando o bastion host cai, a conexão entre a rede interna e externa deixa de funcionar.

As principais **funcionalidades oferecidas pelos firewalls são**:

- **regular o tráfego de dados** entre uma rede local e a rede externa não confiável, por meio da introdução de filtros para pacotes ou aplicações;
- **impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados** dentro de uma rede local;
- mecanismo de **defesa que restringe o fluxo de dados entre redes**, podendo criar um "log" do tráfego de entrada e saída da rede;
- **proteção de sistemas vulneráveis ou críticos**, ocultando informações de rede como nome de sistemas, topologia da rede, identificações dos usuários etc.

A seguir, alguns exemplos de situações que um firewall **NÃO** poderá impedir:

Vírus de E-mail	Os vírus de e-mail são anexos às mensagens de e-mail. Segundo Microsoft (2013), **o firewall NÃO pode determinar o conteúdo das mensagens e, portanto, não pode protegê-lo contra esses tipos de vírus.** Você deve usar um programa antivírus para examinar e excluir anexos suspeitos de uma mensagem de e-mail antes de abri-la. Mesmo tendo um programa antivírus, você não deve abrir um anexo de e-mail se não estiver completamente certo de que ele é seguro.
Tentativas de Phishing	**Phishing** é uma técnica usada para induzir usuários de computador a revelar informações pessoais ou financeiras, como uma senha de conta bancária. Uma tentativa de phishing online comum começa com um e-mail recebido de uma fonte aparentemente confiável, mas que, na verdade, orienta os destinatários a fornecerem informações para um site fraudulento. **O firewall NÃO pode determinar o conteúdo das mensagens de e-mail** e, portanto, **NÃO** pode protegê-lo contra esse tipo de ataque (Microsoft, 2013).

O firewall não tem a função de procurar por ataques. Ele realiza a filtragem dos pacotes e, então, bloqueia as transmissões não permitidas. Dessa forma, atua entre a rede externa e interna, controlando o tráfego de informações que existem entre elas, procurando certificar-se de que este tráfego é confiável, em conformidade com a política de segurança do site acessado. Também pode ser utilizado para atuar entre redes com necessidades de segurança distintas. **Também, o firewall não é antivírus nem antispyware.**

Firewall (pessoal): software que controla o acesso e as comunicações **entre um computador e a Internet ou uma rede local**. Bloqueia hackers e outros tráfegos não autorizados e permite o tráfego autorizado.

Firewall (rede): um dispositivo de hardware, software ou ambos que controla o acesso à rede e as comunicações **entre uma rede e a Internet ou entre duas partes diferentes de uma rede**.

DMZ - Zona Desmilitarizada

Também chamada de **Rede de Perímetro**. Trata-se de uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a Internet.

A função de uma **DMZ** é **manter todos os serviços que possuem acesso externo (navegador, servidor de e-mails) separados da rede local** limitando o dano em caso de comprometimento de algum serviço nela presente por algum invasor. Para atingir este objetivo os computadores presentes em uma DMZ não devem conter nenhuma rota de acesso à rede local.

O termo possui uma origem militar, significando a área existente entre dois inimigos em uma guerra.

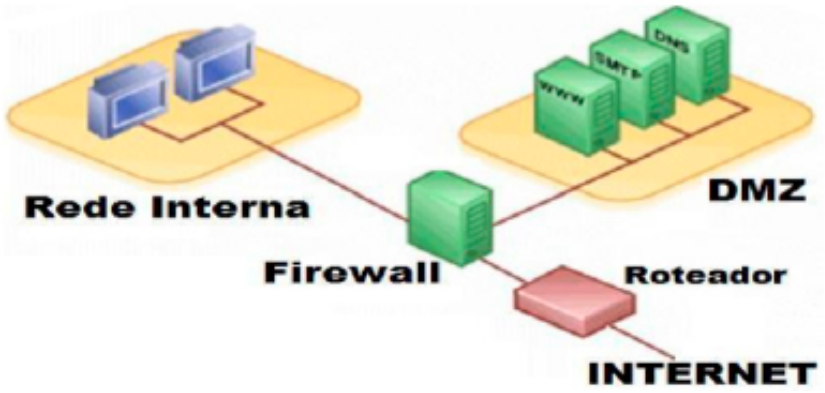


Figura. DMZ

Proxy

É um servidor que atua como um **intermediário** entre a estação de trabalho e a Internet **realizando filtros nos acessos da Internet**. Também guarda informações sobre as páginas visitadas anteriormente em cache.

Normalmente, a comunicação com um proxy utiliza o protocolo HTTP. Também deve ser definida uma porta de comunicação, já que um proxy recebe e envia dados por uma porta específica.

Honeypot = "Pote de Mel"

É um sistema que possui falhas de segurança reais ou virtuais, colocadas de **maneira proposital**, a fim de que seja invadido e que o fruto desta invasão possa ser estudado.

Um honeypot é um recurso de rede cuja função é de ser atacado e compremetido (invadido). Significa dizer que um Honeypot poderá ser testado, atacado e invadido. Os honeypots não fazem nenhum tipo de prevenção, os mesmos fornecem informações adicionais de valor inestimável (Lance Spitzner/2003).

Não possui dados ou aplicações importantes para a organização.

Objetivo: passar-se por equipamento legítimo. Não existem falsos positivos pois o tráfego é real.

RESUMO

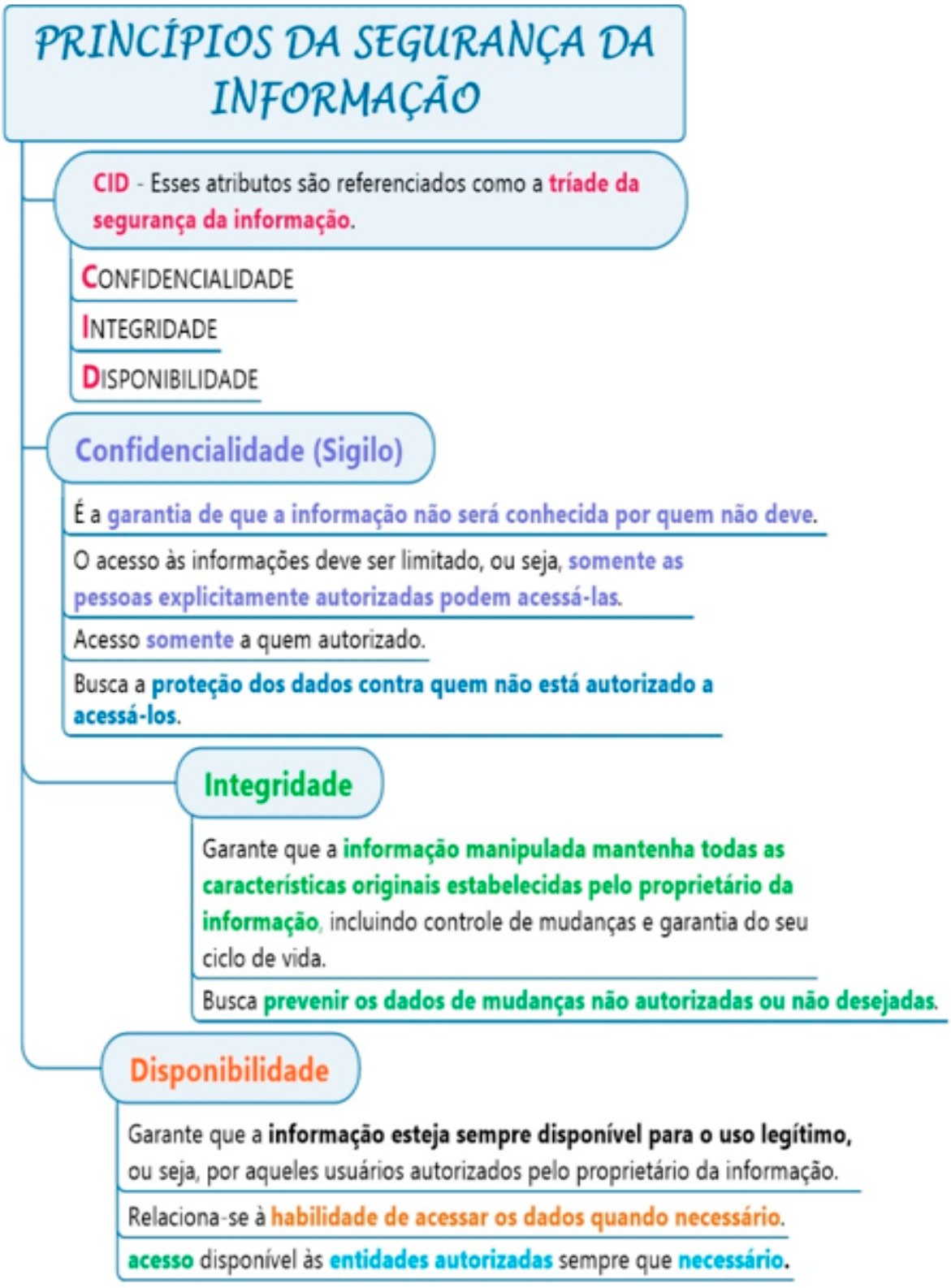


Figura. Princípios da Segurança da Informação. Fonte: Quintão (2020)

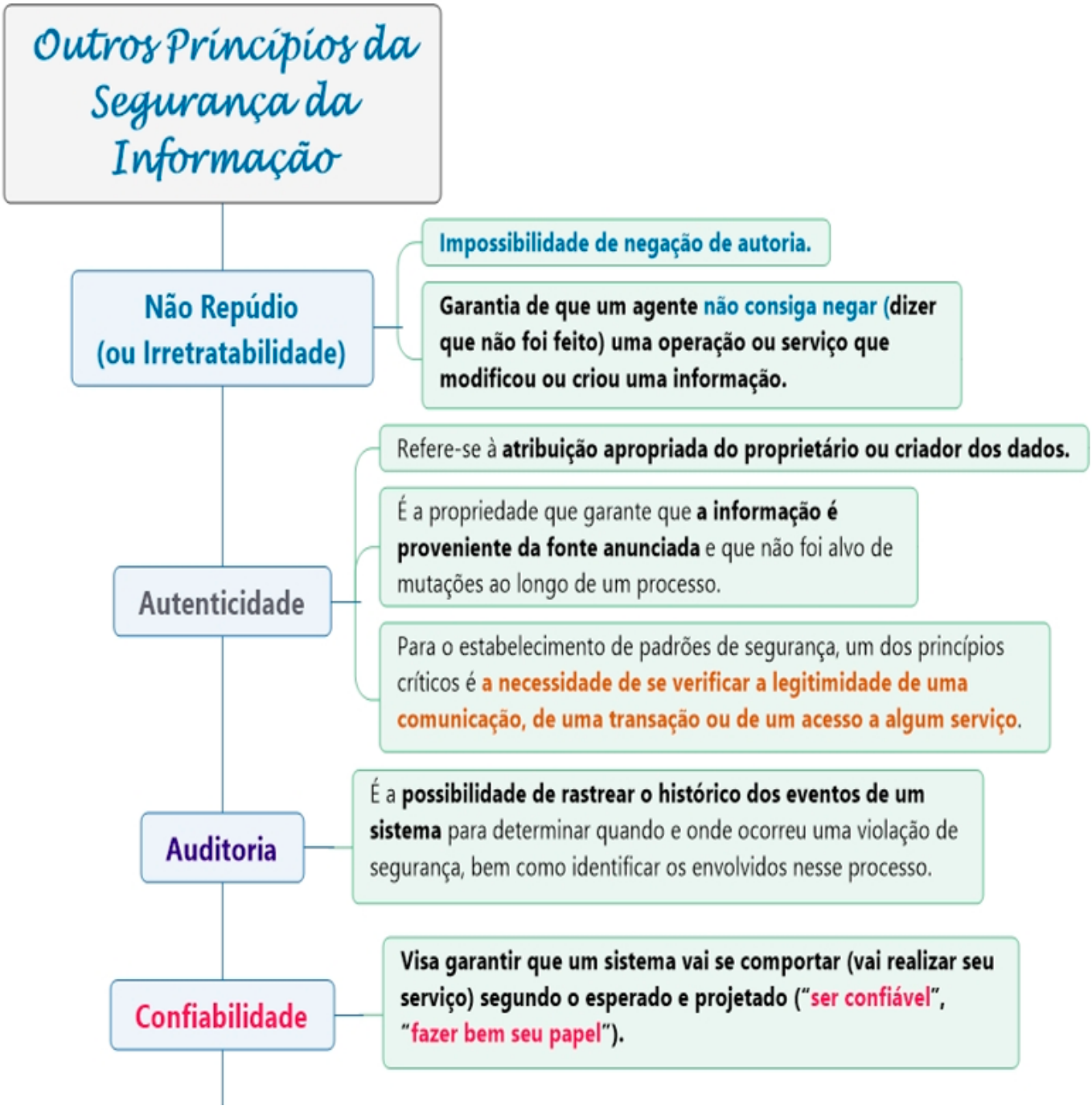


Figura. Outros Princípios da Segurança da Informação. Fonte: Quintão (2020)

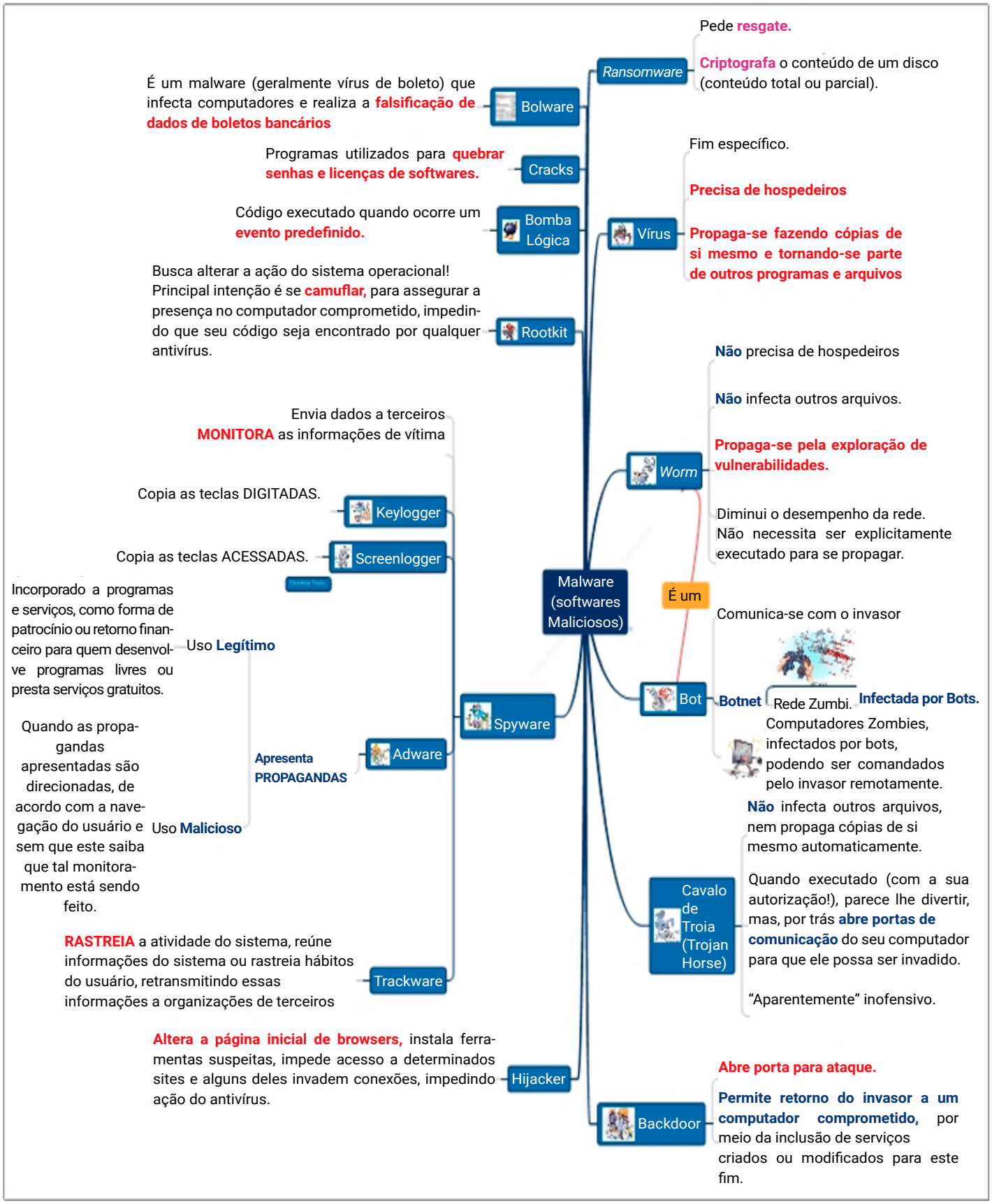


Figura. Malware. Fonte: Quintão (2020)

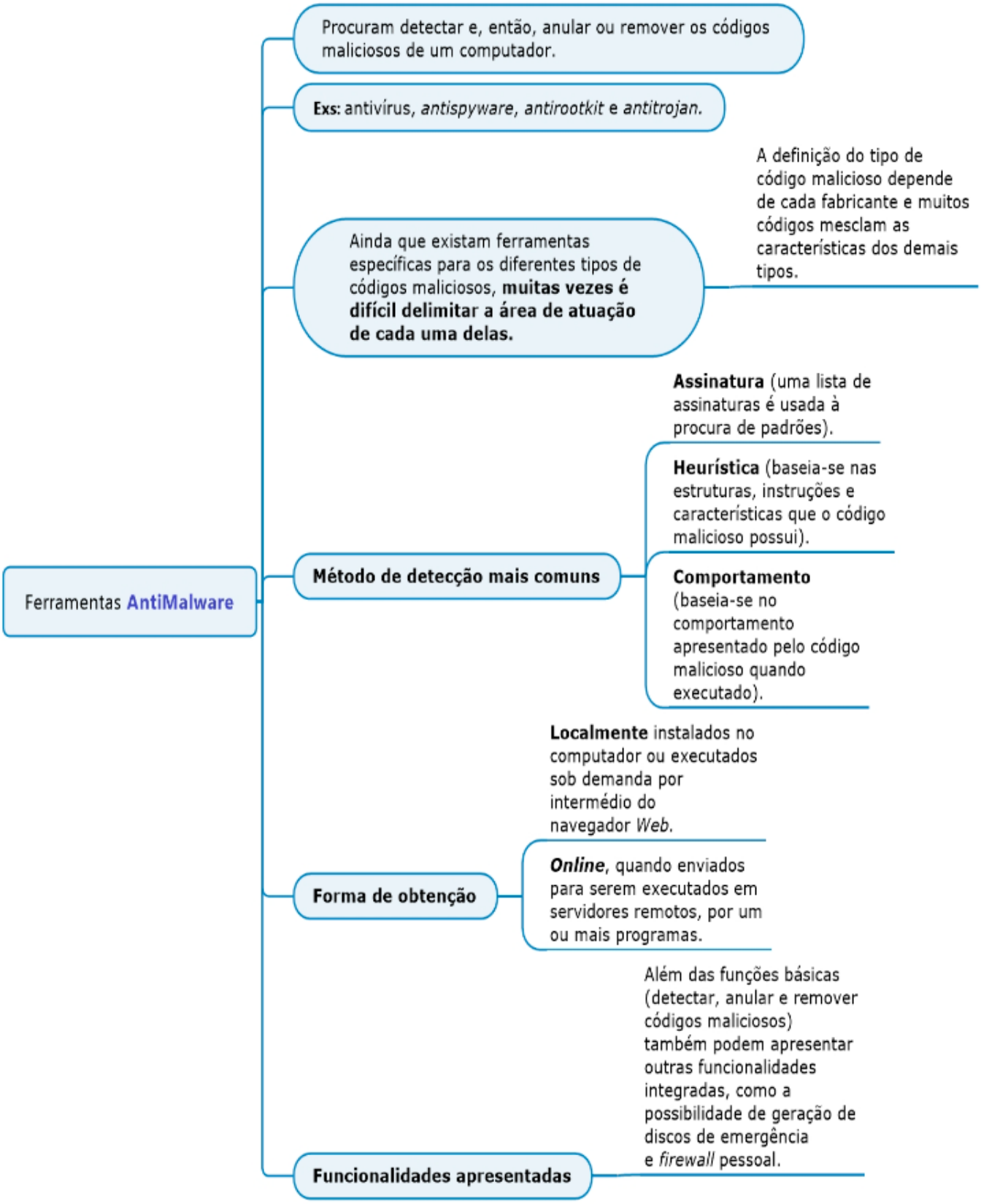


Figura. Ferramentas AntiMalware. Fonte: Quintão (2020)

BACKUPs

CÓPIAS DE SEGURANÇA

MÉTODOS

- online
  com os sistemas em execução
- offline

ATRIBUTOS DOS ARQUIVOS

! ALT + ENTER

informações associadas a **arquivos e pastas** | definem comportamento do **sistema de arquivos**

☑ O ARQUIVO ESTÁ PRONTO PARA SER ARQUIVADO (= arquivo morto)

atributo marcado significa que o arquivo/pasta será copiado no próximo backup

! CAI MTO TIPOS | TÉCNICAS

NORMAL (completo – full)

- copia **todos os arquivos e pastas** selecionados
- desMarca o atributo de arquivamento
- utilizado na criação do **primeiro backup**
- **restauração mais rápida** (somente um backup será restaurado)

INCREMENTAL

- copia **somente os arquivos criados ou alterados** após último backup normal ou incremental
- desMarca o atributo de arquivamento (limpa marcadores)
- backup mais rápido
- **restauração mais demorada** (último backup completo + incrementais anteriores)

DIFERENCIAL

- copia **somente os arquivos criados ou alterados** após último backup normal
- Não desmarca o atributo de arquivamento
- é **cumulativo**
- backup mais demorado
- **restauração mais rápida** (último completo + diferencial)

Figura. Backups (Cópias de Segurança). Fonte: Clube dos Mapas por @paola.tuzani.

QUESTÕES DE CONCURSO

Questão 1 (CESPE/SEFAZ-RS/AUDITOR-FISCAL DA RECEITA ESTADUAL/BLOCO I/2019) Julgue os itens a seguir, acerca de segurança da informação.

I – São exemplos de ameaças as contas sem senhas ou configurações erradas em serviços DNS, FTP e SMTP.

II – Não repúdio indica que o remetente de uma mensagem não deve ser capaz de negar que enviou a mensagem.

III – Vulnerabilidade é a fragilidade de um ativo ou de um grupo de ativos que pode ser explorada.

IV – Pessoas não são consideradas ativos de segurança da informação.

Estão certos apenas os itens

a) I e III.

b) I e IV.

c) II e III.

d) I, II e IV.

e) II, III e IV.

Questão 2 (CESPE/PRF/2019) No acesso a uma página web que contenha o código de um vírus de script pode ocorrer a execução automática desse vírus, conforme as configurações do navegador.

Questão 3 (CESPE/SEFAZ-RS/AUDITOR-FISCAL DA RECEITA ESTADUAL/BLOCO I/2019) Para o estabelecimento de padrões de segurança, um dos princípios críticos é a necessidade de se verificar a legitimidade de uma comunicação, de uma transação ou de um acesso a algum serviço. Esse princípio refere-se à

a) confidencialidade.

b) autenticidade.

c) integridade.

d) conformidade.

e) disponibilidade.

Questão 4 (CESPE/BNB/ANALISTA BANCÁRIO/2018) Acerca de pesquisas na Web e de vírus e ataques a computadores, julgue o item subsequente.

Entre as categorias de antivírus disponíveis gratuitamente, a mais confiável e eficiente é o scareware, pois os antivírus dessa categoria fazem uma varredura nos arquivos e são capazes de remover 99% dos vírus existentes

Questão 5 (CESPE/BNB/ANALISTA BANCÁRIO/2018) Acerca de pesquisas na Web e de vírus e ataques a computadores, julgue o item subsequente.

Se um rootkit for removido de um sistema operacional, esse sistema não voltará à sua condição original, pois as mudanças nele implementadas pelo rootkit permanecerão ativas.

Questão 6 (CESPE/POLÍCIA FEDERAL/PAPILOSCOPISTA POLICIAL FEDERAL/2018)

No que se refere à segurança de computadores, julgue o item subsecutivo. Cavalos de Troia são exemplos de vírus contidos em programas aparentemente inofensivos e sua ação danosa é mascarada pelas funcionalidades do hospedeiro.

Questão 7 (CESPE/POLÍCIA FEDERAL/AGENTE DA POLÍCIA FEDERAL/2018) Julgue o próximo item, a respeito de proteção e segurança, e noções de vírus, worms e pragas virtuais.

A infecção de um sistema por códigos maliciosos pode ocorrer por meio da execução de arquivos infectados obtidos de anexos de mensagens eletrônicas, de mídias removíveis, de páginas web comprometidas, de redes sociais ou diretamente de outros equipamentos.

Questão 8 (CESPE/POLÍCIA FEDERAL/ESCRIVÃO DE POLÍCIA FEDERAL/2018)

Acerca de redes de computadores e segurança, julgue o item que segue.

Os aplicativos de antivírus com escaneamento de segunda geração utilizam técnicas heurísticas para identificar códigos maliciosos.

Questão 9 (CESPE/PC-MA/2018) Julgue o item subsequente, relativo a software para o ambiente de microinformática e a proteção e segurança da informação.

Fazer becape regularmente é uma conduta que permite minimizar os danos decorrentes de um ataque do tipo ransomware locker, que impede o acesso ao equipamento infectado, visto que o pagamento do resgate não garante acesso aos dados.

Questão 10 (CESPE/PM-MA/2018) A seguir são apresentadas três situações hipotéticas.

I – Um usuário, após sequestro de seus dados, recebeu a informação de que, para reavê-los, seria necessário realizar um pagamento ao sequestrador.

II – Um usuário recebeu informação, por meio do setor de segurança da informação do seu órgão, de que seu computador, sem seu conhecimento, havia sido usado em um ataque a uma rede de outro órgão.

III – Em um dado momento do dia, um usuário notou que sua máquina estava consumindo mais recursos de memória do que o habitual e, ao executar no computador um programa de proteção, obteve a seguinte mensagem: "arquivo xpto infectado com o worm xyz".

Com referência a essas situações hipotéticas e à segurança da informação, julgue o item subsequente.

A situação III caracteriza-se mais como vírus do que como um worm, pois os vírus são responsáveis por consumir muitos recursos, ao passo que os worms permitem o retorno de um invasor ao computador comprometido.

Questão 11 (CESPE/TCE-PB/2018) Entre os vários tipos de programas utilizados para realizar ataques a computadores, aquele capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo entre computadores, é conhecido como

a) botnet.

b) spyware.

c) backdoor.

d) trojan.

e) worm.

Questão 12 (CESPE/PC-MA/ESCRIVÃO DE POLÍCIA/2018) Determinado tipo de vírus eletrônico é ativado quando um documento por ele infectado é aberto, podendo então, nesse momento, infectar não apenas outros documentos, mas também um gabarito padrão de documento, de modo que cada novo documento criado sob esse gabarito seja infectado. Tal vírus, cuja propagação ocorre quando documentos por ele infectados são remetidos por correio eletrônico para outros usuários, é conhecido como

a) vírus de setor de carga (boot sector).

b) vírus de programa.

c) vírus de macro.

d) backdoor.

e) hoax.

Questão 13 (CESPE/ANVISA/2016) Códigos maliciosos podem ter acesso aos dados armazenados no computador e executar ações em nome dos usuários, de acordo com as permissões de operação de cada um destes.

Questão 14 (CESPE/DPU/ANALISTA/2016) A respeito da Internet e suas ferramentas, julgue o item a seguir.

Malwares são mecanismos utilizados para evitar que técnicas invasivas, como phishing e spams, sejam instaladas nas máquinas de usuários da Internet.

Questão 15 (CESPE/INSS/TÉCNICO DO INSS/2016) A infecção de um computador por vírus enviado via correio eletrônico pode se dar quando se abre arquivo infectado que porventura esteja anexado à mensagem eletrônica recebida.

Questão 16 (CESPE/INSS/ANALISTA DO SEGURO SOCIAL COM FORMAÇÃO EM SERVIÇO SOCIAL/2016) Cada um dos próximos itens, que abordam procedimentos de informática e conceitos de Internet e intranet, apresenta uma situação hipotética, seguida de uma assertiva a ser julgada.

Ao iniciar seu dia de trabalho, Daniel se deparou com inúmeros aplicativos abertos em seu computador de trabalho, o que deixava sua máquina lenta e sujeita a travamentos frequentes. Ele constatou, ainda, que somente um desses aplicativos era necessário para a execução de suas atividades.

Nessa situação, para melhorar o desempenho do seu computador, Daniel deve utilizar um aplicativo de antivírus instalado localmente, para eliminar os aplicativos que estiverem consumindo recursos além do normal.

Questão 17 (CESPE/DPU/ANALISTA/2016) A respeito da Internet e suas ferramentas, julgue o item a seguir.

Integridade, confidencialidade e disponibilidade da informação, conceitos fundamentais de segurança da informação, são adotados na prática, nos ambientes tecnológicos, a partir de um conjunto de tecnologias como, por exemplo, criptografia, autenticação de usuários e equipamentos redundantes.

Questão 18 (CESPE/TRE-PI/CONHECIMENTOS GERAIS PARA OS CARGOS 1, 2 E 4/2016) A remoção de códigos maliciosos de um computador pode ser feita por meio de

a) anti-spyware.

b) detecção de intrusão.

c) anti-spam.

d) anti-phishing.

e) filtro de aplicações.

Questão 19 (CESPE/TRE-RS/TÉCNICO JUDICIÁRIO/CONHECIMENTOS BÁSICOS PARA OS CARGOS 6 A 8/2015) Em relação a vírus, worms e pragas virtuais, assinale a opção correta.

a) Para garantir a segurança da informação, é suficiente instalar e manter atualizados antivírus.

b) Não há diferença — seja conceitual, seja prática — entre worms e vírus; ambos são arquivos maliciosos que utilizam a mesma forma para infectar outros computadores.

c) Rootkits é um arquivo que infecta o computador sem causar maiores danos, ainda que implique a pichação da tela inicial do navegador.

d) A segurança da informação em uma organização depende integralmente de a sua área de tecnologia optar pela adoção de recursos de segurança atualizados, como firewall e antivírus.

e) Em segurança da informação, denominam-se engenharia social as práticas utilizadas para obter acesso a informações importantes ou sigilosas sem necessariamente utilizar falhas no software, mas, sim, mediante ações para ludibriar ou explorar a confiança das pessoas.

Questão 20 (CESPE/TELEBRAS/ANALISTA SUPERIOR/COMERCIAL/2015) A respeito de segurança da informação, julgue o item subsecutivo.

Worms, assim como os vírus, são autorreplicáveis e necessitam ser executados pelos usuários para se propagarem e infectarem os computadores de uma rede.

Questão 21 (CESPE/TCE-RN/CONHECIMENTOS BÁSICOS PARA OS CARGOS 2 E 3/2015) Julgue o item subsequente, a respeito de organização e gerenciamento de arquivos, pastas e programas, bem como de segurança da informação.

A principal diferença entre crackers e hackers refere-se ao modo como esses malfeitores da área de segurança da informação atacam: os crackers são mais experientes e realizam ataques sem utilizar softwares, ao passo que os hackers utilizam códigos maliciosos associados aos softwares para realizar ataques ao ciberespaço.

Questão 22 (CESPE/TJ-DFT/ANALISTA JUDICIÁRIO/CONHECIMENTOS BÁSICOS PARA OS CARGOS 2, 3 E 5 A 12/2015) Com relação a redes de computadores, Internet e respectivas ferramentas e tecnologias, julgue o item a seguir.

Na segurança da informação, controles físicos são soluções implementadas nos sistemas operacionais em uso nos computadores para garantir, além da disponibilidade das informações, a integridade e a confidencialidade destas.

Questão 23 (CESPE/TRE-MT/TÉCNICO JUDICIÁRIO/ CONHECIMENTOS GERAIS PARA O CARGO 6/2015) A função principal de uma ferramenta de segurança do tipo antivírus é

a) monitorar o tráfego da rede e identificar possíveis ataques de invasão.

b) verificar arquivos que contenham códigos maliciosos.

c) fazer becape de segurança dos arquivos considerados críticos para o funcionamento do computador.

d) bloquear sítios de propagandas na Internet.

e) evitar o recebimento de mensagens indesejadas de e-mail, tais como mensagens do tipo spams.

Questão 24 (CESPE/TJ-DFT/ANALISTA JUDICIÁRIO/CONHECIMENTOS BÁSICOS PARA OS CARGOS 2, 3 E 5 A 12/2015) A respeito de sistemas operacionais e aplicativos para edição de texto, julgue o item que se segue. Vírus do tipo boot, quando instalado na máquina do usuário, impede que o sistema operacional seja executado corretamente.

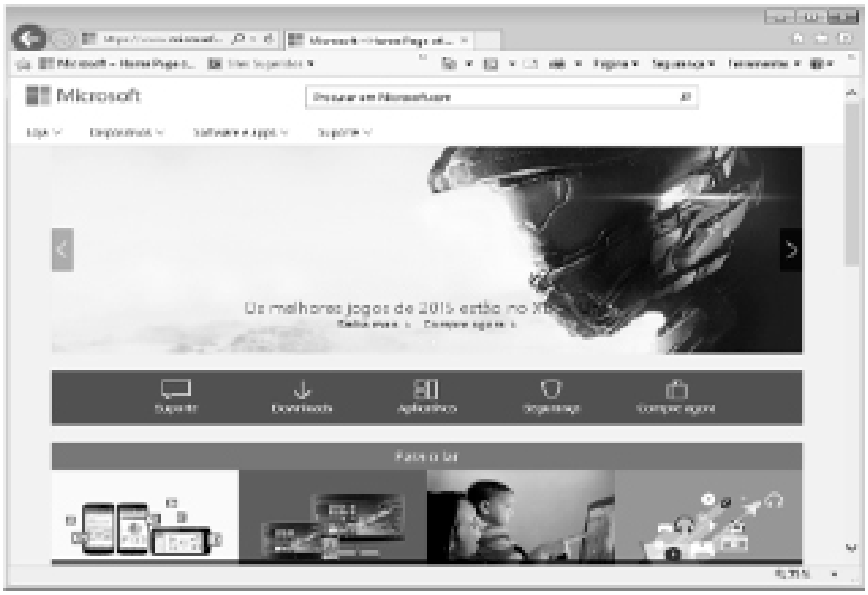
Questão 25 (CESPE/TELEBRAS/ANALISTA ADMINISTRADOR/ CONHECIMENTOS BÁSICOS PARA O CARGO 3/2015) No que se refere à segurança da informação, julgue o seguinte item.

Sniffers são programas aparentemente inofensivos cuja principal característica é utilizar a técnica de mascaramento. A técnica em questão permite, por exemplo, que um sniffer seja anexado a um jogo, que, por sua vez, ao ser instalado em um computador, coletará informações bancárias do usuário.

Questão 26 (CESPE/TELEBRAS/ANALISTA SUPERIOR/COMERCIAL/2015) A respeito de segurança da informação, julgue o item subsecutivo.

Uma das formas de manter o aparelho de telefone celular livre de vírus é deixar o bluetooth habilitado constantemente, para que ele possa identificar possíveis anexos maliciosos às mensagens recebidas.

Questão 27 (CESPE/CEBRASPE/MP-ENAP/ADMINISTRADOR CARGO 1/2015)



A respeito da figura acima apresentada, do Internet Explorer 11 e de segurança da informação, julgue o item a seguir.

Trackwares são programas que rastreiam a atividade do sistema, reúnem informações do sistema ou rastreiam os hábitos do usuário, retransmitindo essas informações a organizações de terceiros.

Questão 28 (CESPE/TRE-GO/ANALISTA JUDICIÁRIO/2015) Acerca de procedimentos de segurança e de ensino a distância, julgue o item subsecutivo. [Botnet é uma rede formada por inúmeros computadores zumbis e que permite potencializar as ações danosas executadas pelos bots, os quais são programas similares ao worm e que possuem mecanismos de controle remoto].

Questão 29 (CESPE/TRE-GO/ANALISTA JUDICIÁRIO/2015) Acerca de procedimentos de segurança e de ensino a distância, julgue o item subsecutivo. Quanto à segurança da informação, sugere-se que se crie um disco de recuperação do sistema, assim como se desabilite a autoexecução de mídias removíveis e de arquivos anexados.

Questão 30 (CESPE/CADE/NÍVEL INTERMEDIÁRIO/NÍVEL MÉDIO/2014) Acerca dos conceitos de gerenciamento de arquivos e de segurança da informação, julgue o item subsequente. O computador utilizado pelo usuário que acessa salas de bate-papo não está vulnerável à infecção por worms, visto que esse tipo de ameaça não se propaga por meio de programas de chat.

Questão 31 (FCC/TRT-14ª REGIÃO/RO E AC/ANALISTA JUDICIÁRIO/ESTATÍSTICA/2018) Crime cibernético é todo crime que é executado online e inclui, por exemplo, o roubo de informações no meio virtual. Uma recomendação correta de segurança aos usuários da internet, para se proteger contra a variedade de crimes cibernéticos é

a) usar a mesma senha (composta por letras maiúsculas e minúsculas, números e símbolos) em todos os sites com conteúdo de acesso restrito, mantendo esta senha protegida em um aplicativo de gerenciamento de senhas.

b) manter os softwares atualizados, exceto os sistemas operacionais, pois estes já possuem mecanismos de segurança como firewall, antivírus e antispyware.

c) gerenciar as configurações de mídias sociais para manter a maior parte das informações pessoais e privadas bloqueadas.

d) proteger a rede wireless com senha que utiliza criptografia Wired Equivalent Privacy – WEP ou com uma Virtual Protect Network – VPN.

e) usar uma suíte de segurança para a internet com serviços como firewall, blockwall e antivírus, como o LibreOffice Security Suit.

Questão 32 (FCC/SEGEP-MA/2018) Em uma situação hipotética, um funcionário da Secretaria de Estado da Gestão e Assistência dos Servidores (SEGEP) verificou que um tipo de código malicioso (malware) havia invadido e tornado inacessíveis os dados armazenados em seu equipamento porque tudo havia sido criptografado. O invasor exigiu pagamento de resgate para restabelecer o acesso.

Essa situação mostra a ocorrência do ataque cibernético de um malware conhecido por:

a) Spam.

b) Ransomware.

c) Trojan Spy.

d) Cookie.

e) Worm.

Questão 33 (FCC/AGED-MA/2018) Não importa se um usuário utiliza Microsoft, MacOS, Android ou outro tipo de sistema operacional, pois ao se conectar na internet com um deles, já fica vulnerável a uma infinidade de ataques digitais e pode sofrer com um tipo de malware cuja invasão é realizada com o intuito de causar algum dano ou roubar informações.

(Adaptado de: http://tecnologia.ig.com.br/2017-04-04/malware-cimes-ciberneticos.html)

O malware referenciado no texto é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções maliciosas sem o conhecimento do usuário. Ataca através de programas que necessitam ser explicitamente executados para que sejam instalados, mas também pode ser instalado por atacantes que, após invadirem o computador, alteram programas já existentes para que também executem ações maliciosas. Este malware e denominado:

a) worm.

b) rootkit.

c) trojan.

d) wanna cry.

e) ransomware

Questão 34 (FCC/ALESE/TÉCNICO LEGISLATIVO/TÉCNICO-ADMINISTRATIVO/2018) Uma ação que NÃO potencializa o risco de golpes (scam) na Internet e de infecção de computador por malware é

a) baixar atualizações ou softwares em sites de acesso mais rápido que o do fabricante.

b) entrar em sites para baixar uma faixa musical, álbum ou filmes sem pagar.

c) utilizar a mesma senha complexa em todos os sites que possui cadastro.

d) utilizar Virtual Private Network confiável para acessar a Internet em locais públicos.

e) abrir arquivos anexos no webmail, quando o assunto indicar alta prioridade.

Questão 35 (FCC/METRÔ-SP/OFICIAL LOGÍSTICA ALMOXARIFADO I/2018) O usuário de um computador deu um duplo clique sobre um programa recebido por e-mail, executando-o, e seu computador foi infectado por um malware que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e/ou arquivos. Tais características permitem concluir que o computador foi infectado por um

a) warm.

b) vírus.

c) rootkit.

d) botnet.

e)backdoor.

Questão 36 (FCC/SEGEP-MA/AUXILIAR DE FISCALIZAÇÃO AGROPECUÁRIA/2018) Ataques cibernéticos causaram prejuízo de US$ 280 bilhões às corporações

A extorsão virtual, quando servidores de empresas são bloqueados e seus gestores só recebem acesso novamente mediante pagamento para os criminosos, também é um dos maiores problemas na América Latina, 28,1%, ficando atrás apenas do bloco de países Asiáticos, 35,1%. Os setores mais suscetíveis a essa modalidade de ataques cibernéticos são serviços financeiros (45,8%); cuidados da saúde (23,7%); energia (23,3%); bens de consumo (22,4%); educação (22,1%); viagem, turismo e lazer (19,8%); agricultura (17,9%); setor produtivo (16,3%);

tecnologia, meios de comunicação e telecomunicações (13,0%); transporte (11,3%); imobiliário e construção (6,2%) e serviços profissionais (4,8%).

(Disponível em: http://www.convergenciadigital.com.br)

O texto se refere à "extorsão virtual, quando servidores de empresas são bloqueados e seus gestores só recebem acesso novamente mediante pagamento para os criminosos" e quase 18% deste tipo de ataque atinge o setor de agricultura. A denominação deste tipo de ataque é

a) bot.

b) spyware.

c) backdoor.

d) ransomware.

e) rootkit.

Questão 37 (FCC/TRE-SP/ANALISTA JUDICIÁRIO/ÁREA ADMINISTRATIVA/2017) Considere o texto abaixo.

Com efeito, nesse tipo específico de delito, o agente obtém, para ele ou outrem, vantagem ilícita (numerário subtraído de conta bancária), em prejuízo de alguém (a vítima, cliente de banco) mediante o emprego do artifício da construção de uma página eletrônica falsa ou envio de mensagem eletrônica (e-mail) de conteúdo fraudulento. Não haveria, como se disse, qualquer dificuldade de enquadramento do praticante do "ato ilícito" no art. 171 do CPC, impondo-lhe as sanções previstas nesse dispositivo (reclusão, de um a cinco anos, e multa). Além do mais, quando o criminoso implementa o último estágio da execução ilícita, que é a subtração não autorizada dos fundos existentes na conta da vítima, a jurisprudência tem entendido que aí está caracterizado o crime de furto qualificado, previsto no art. 155, § 4º, II.

(Adaptado de: REINALDO FILHO, Democrito. Disponível em: http://www.teleco.com.br/pdfs/tutorialintbank.pdf)

Hipoteticamente, um Analista Judiciário do TRE-SP identificou, corretamente, o ato ilícito referido entre aspas no texto como um tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. Comumente realizado por meio da internet, esse golpe é caracterizado como

a) identity theft.

b) fielding.

c) phishing.

d) hacker.

e) worming.

Questão 38 (FCC/ALESE/TÉCNICO LEGISLATIVO/TÉCNICO-ADMINISTRATIVO/2018)

Considere o trecho a seguir, retirado do Relatório de Crimes Cibernéticos da empresa Norton:

Vírus de computador e ataques de malware são os tipos mais comuns de crime cibernético que as pessoas sofrem, com 51% dos adultos sentindo os efeitos desses crimes mundialmente. Na Nova Zelândia, Brasil e China é ainda pior, com mais de 6 em 10 computadores infectados (61%, 62% e 65%, respectivamente). Os adultos em todo o mundo também são alvos de golpes (scams) online, ataques de phishing, roubo de perfis de redes sociais e fraude de cartão de crédito. 7% dos adultos até mesmo se depararam com predadores sexuais online.

(Disponível em: http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Portuguese-Hu man%20Impact-A4_Aug18.pdf)

O phishing, mencionado no texto, é um tipo de golpe por meio do qual um golpista

a) faz varreduras na rede do usuário, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles.

b) tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

c) armazena tudo o que o usuário digita pelo teclado do computador e depois obtém estes dados remotamente.

d) altera campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

e) utiliza um computador ou dispositivo móvel para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

Questão 39 (FCC/ISS-TERESINA/AUDITOR FISCAL DO MUNICÍPIO/TI/2016) Um funcionário de uma empresa percebeu que seu computador estava sendo controlado remotamente sem seu consentimento, quando foi notificado pelo administrador da rede que, a partir de seu computador, estavam sendo enviados spams, realizados ataques de negação de serviço e pro-

pagação de outros códigos maliciosos. Com base nestas características e ações, conclui-se que o computador deve estar infectado por um

a) vírus.

b) rootkit.

c) keylogger.

d) spyware.

e) bot.

Questão 40 (FCC/TRE-PB/TÉCNICO JUDICIÁRIO/ÁREA ADMINISTRATIVA/2015) Atualmente, a forma mais utilizada para a disseminação de vírus é por meio de mensagens de e-mails com anexos recebidos pela internet. Para que o vírus seja ativado:

a) é necessária a transferência do anexo para a Área de trabalho do computador.

b) é necessário que o anexo contaminado seja aberto ou executado.

c) basta realizar a abertura da mensagem para a sua leitura.

d) é suficiente o download da mensagem do servidor de e-mail para o computador.

e) é necessário que, uma vez aberta a mensagem, haja uma conexão com a internet.

Questão 41 (FCC/TRE-RR/ANALISTA JUDICIÁRIO/MEDICINA/2015) O processo de proteção da informação das ameaças caracteriza-se como Segurança da Informação. O resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco aspectos principais:

I – Somente as pessoas autorizadas terão acesso às informações.

II – As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.

III – Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

IV – Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

V – Garante que as informações foram produzidas respeitando a legislação vigente.

Os aspectos elencados de I a V correspondem, correta e respectivamente, a:

a) integridade - disponibilidade - confidencialidade - autenticidade –legalidade.

b) disponibilidade - confidencialidade - integridade - legalidade -autenticidade.

c) confidencialidade - integridade - disponibilidade - autenticidade -legalidade.
d) autenticidade - integridade - disponibilidade - legalidade –confidencialidade.
e) autenticidade - confidencialidade - integridade - disponibilidade -legalidade.

Questão 42 (FCC/CNMP/ANALISTA DO CNMP/SUPORTE E INFRAESTRUTURA/2015) Alguns programas antivírus colocam arquivos suspeitos de possuírem vírus em quarentena, pelo fato de que não terem como combatê-los nesse momento. Um cuidado que o usuário do computador deve ter a partir de então, seguindo as recomendações dos programas antivírus, é de
a) reinstalar o sistema operacional, pois o possível vírus pode tê-lo contaminado, e não existem formas de reverter essa situação.
b) adquirir e instalar uma extensão do programa antivírus específica para o problema identificado.
c) apagar do computador todos os arquivos com a mesma extensão do arquivo colocado em quarentena, pois podem ter sido contaminados.
d) manter o programa antivírus sempre atualizado, na expectativa de que esse possível vírus possa ser identificado, e formas de combatê-lo desenvolvidas e incorporadas ao programa antivírus.
e) reinicializar o computador para que todos os efeitos desse possível vírus sejam anulados.

Questão 43 (FCC/TCE-CE/ANALISTA DE CONTROLE EXTERNO/AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO/2015) Após o exame no computador do funcionário de uma instituição foi detectada sua participação em um ataque de DDoS sem seu conhecimento, em que seu computador atuava como um "zumbi", controlado remotamente por um atacante. Isso ocorreu porque o computador estava infectado por
a) adware.
b) rootkit.
c) bot.
d) spyware.
e) trojan.

Questão 44 (FCC/TRT-15/CAMPINAS-SP/ANALISTA JUDICIÁRIO/TI/2015) Sobre um programa de código malicioso – malware, considere:

I – É notadamente responsável por consumir muitos recursos devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho de redes e a utilização de computadores.

II – Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

III – Diferente do vírus, não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Os itens I, II e III tratam de características de um

a) Trojan Proxy.

b) Keylogger.

c) Scan.

d) Worm.

e) Spoofing.

Questão 45 (FCC/ALEPE/AGENTE LEGISLATIVO/2014) Um usuário fez o download de um programa gratuito para obter vídeos da Internet. Imediatamente após instalar o programa, o usuário notou que o seu navegador web passou a remetê-lo para a página inicial de um site indesejado, cheio de propagandas e informações sobre prêmios, sendo que essa página solicita de imediato alguns dados pessoais do internauta. Ele reeditou a informação da página inicial do seu navegador, eliminando a página indesejada e substituindo-a pela de sua preferência. Surpreendentemente, a cada vez que o navegador era reiniciado ou quando era selecionada a abertura de uma nova página da Internet, o site indesejado voltava a ser exibido. Esse tipo de ocorrência refere-se a um

a) spyware, que está espionando a navegação do usuário com o objetivo de gerar informações relevantes para um hacker através da página redirecionada, que permitirá ao hacker o bloqueio remoto das ações do usuário.

b) trojan ou cavalo de tróia, que pode ter sido obtido no momento do download da aplicação para obter vídeos e em seguida ter sido executado pelo internauta.

c) sniffer, que tem por objetivo remeter o internauta para uma página web na qual onde os dados que ele digitar serão capturados por um cracker.

d) phishing, que falsifica a página principal do navegador, remetendo o internauta para outro endereço na internet.

e) worm hospedado no software que foi objeto de download, o qual tem por objetivo enviar os arquivos do usuário para um local na Internet acessado por um hacker.

Questão 46 (FCC/ICMS-RJ/AUDITOR-FISCAL DA RECEITA ESTADUAL/2014) A política de segurança da informação da Receita Estadual inclui um conjunto de diretrizes que determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações. Dentre estas diretrizes encontram-se normas que garantem

I – a fidedignidade de informações, sinalizando a conformidade dos dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinalizam, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário, garantindo a não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.

II – que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, assegurando a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.

III – que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio das redes de comunicação, assegurando que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento.

Em relação às informações, as normas definidas em I, II e III visam garantir

a) fidedignidade, acessibilidade e disponibilidade.

b) integridade, disponibilidade e confidencialidade.

c) confidencialidade, integridade e autenticidade.

d) integridade, ininterruptibilidade e autenticidade.

e) confidencialidade, integridade e disponibilidade.

Questão 47 (FCC/AL-PE/ANALISTA LEGISLATIVO/INFRAESTRUTURA/2014) Os programas antivírus:

I – Protegem contra phishing de páginas web quando o usuário está em navegação utilizando livremente o browser.

II – Protegem contra trojan embarcado em uma aplicação quando o usuário aceita a sua instalação em sua máquina.

III – Criptografam comunicações em rede, sejam elas por meio de envio de mensagens ou navegação na Internet através de browser.

IV – Protegem contra códigos maliciosos embutidos em macros, as quais são utilizadas por um software aplicativo ou utilitário do computador do usuário.

V – Previnem a instalação de aplicativos infectados, no momento da solicitação de sua instalação, ao gerarem um alerta sobre conteúdo suspeito ou ao bloquearem a operação de instalação.

Está correto o que se afirma APENAS em:

a) I e II.

b) II e III.

c) III e IV.

d) IV e V.

e) II e V.

Questão 48 (FCC/ICMS-RJ/AUDITOR-FISCAL DA RECEITA ESTADUAL/2014) O site Convergência Digital divulgou a seguinte notícia: O Brasil segue como o no 1 na América Latina em atividades maliciosas e figura na 4ª posição mundial, ficando atrás apenas dos EUA, China e Índia, de acordo a Symantec. Os ataques por malwares cresceram 81%.... Um desses malwares segue sendo o grande vilão nas corporações, sendo responsável por mais de 220 milhões de máquinas contaminadas no mundo. É um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

(Adaptado de: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.ht m?infoid=34673&sid=18#.UlqcC-NKsiSo)

Considerando que o malware citado como vilão não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias

ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores, trata-se de um

a) vírus de macro.

b) botnet.

c) worm.

d) spyware.

e) backdoor.

Questão 49 (FCC/TRT-18ª REGIÃO/GO/TÉCNICO JUDICIÁRIO/ TECNOLOGIA DA INFORMAÇÃO/2013) Em relação aos tipos de malware mencionados abaixo, é correto afirmar:

a) Rootkit é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

b) Backdoor é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.

c) Spyware é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes que exploram vulnerabilidades existentes nos programas instalados para invadi-lo.

d) Bot é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. Apesar de ainda serem bastante usados por atacantes, os bots atualmente têm sido também utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção.

e) Trojan ou trojan-horse, é um 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. Estes programas geralmente consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Questão 50 (FCC/TRE-CE/TÉCNICO JUDICIÁRIO/PROGRAMAÇÃO DE SISTEMAS/2012) Sobre segurança da informação, analise:

I – É obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

II – A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída aumenta a eficácia da implementação de um controle de acesso centralizado.

III – Os controles de segurança precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

IV – É importante para os negócios, tanto do setor público como do setor privado, e para proteger as infraestruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (e-gov) ou o comércio eletrônico (e-business), e evitar ou reduzir os riscos relevantes.

Está correto o que consta em

a) I, II, III e IV.

b) I, III e IV, apenas

c) I e IV, apenas.

d) III e IV, apenas.

e) I e II, apenas.

Questão 51 (FCC/TRT-11ª REGIÃO/PROVAS DE ANALISTA JUDICIÁRIO E TÉCNICO JUDICIÁRIO/2012) Quando o cliente de um banco acessa sua conta corrente através da internet, é comum que tenha que digitar a senha em um teclado virtual, cujas teclas mudam de lugar a cada caractere fornecido. Esse procedimento de segurança visa evitar ataques de

a) spywares e adwares.
b) keyloggers e adwares.
c) screenloggers e adwares.
d) phishing e pharming.
e) keyloggers e screenloggers.

Questão 52 (FGV/ALERJ/2017) Ataques cibernéticos podem causar graves prejuízos a pessoas e empresas. Recentemente João recebeu uma mensagem de alerta por e-mail com um pedido para ele atualizar seus dados cadastrais na página do seu Internet Banking.
João não prestou muita atenção em quem enviou a mensagem, nem se era um remetente confiável, e clicou no link presente no corpo do e-mail, que o levou para uma página web, replica do website real criada por um cyber criminoso.
Como a mensagem de e-mail e o website eram muito bem elaborados, João acreditou estar acessando algo verdadeiro e informou suas credenciais para acesso, quando na verdade ele as entregou a um criminoso.
João foi vítima de um ataque cibernético denominado:
a) DDoS;
b) sniffer;
c) spam;
d) phishing;
e) spoofing.

Questão 53 (IADES/SEASTER-PA/TÉCNICO DE ENFERMAGEM/2019) Acerca dos procedimentos de segurança que devem ser adotados ao utilizar-se um computador, assinale a alternativa correta.
a) Não é recomendável utilizar CD-ROM para gravar cópias de arquivos.
b) Cópias de segurança de arquivos confiáveis devem ser feitas, mas somente em servidores on-line.
c) Qualquer arquivo importante deve ser copiado, seja ele confiável ou infectado.
d) Toda cópia de arquivo é confiável.
e) A manutenção de cópias de segurança redundantes de arquivos importantes é recomendável.

Questão 54 (IADES/SEASTER-PA/ENFERMEIRO/2019) Um spyware é um programa desenvolvido para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Com relação a esse assunto, assinale a alternativa correspondente a um programa que pode ser classificado como um spyware.

a) Rootkit
b) Backdoor
c) Adware
d) Vírus
e) Worms

Questão 55 (IADES/CAU–AC/AUXILIAR ADMINISTRATIVO/2019) A internet apresenta diversas ameaças ao usuário, que necessita ter atenção para navegar e não ser afetado. Entre elas, há a ameaça Spam, que pode ser definida como

a) o monitoramento das atividades do e-mail alvo.
b) um programa de computador que se propaga inserindo cópias de si mesmo.
c) a lixeira temporária do servidor de e-mails.
d) um programa instalado que se comunica com o invasor, para que este o controle à distância.
e) o envio não solicitado ou indesejado de e-mails a um grande número de pessoas.

Questão 56 (IADES/APEX BRASIL/ASSISTENTE/2018) O termo malwares, utilizado para se referir a programas maliciosos, nasceu da combinação das palavras, de língua inglesa, malicious e software.

Há um tipo de malware, normalmente recebido como um “presente” (por exemplo, um cartão virtual), que possibilita uma maneira de acesso remoto ao computador após a infecção e, além de executar as funções para as quais foi projetado, executa também outras funções normalmente danosas e sem o conhecimento dos usuários. O malware descrito é denominado de

a) screenlogger.
b) cavalo de Troia.
c) worm.
d) vírus.
e) backdoor.

GABARITO

1. c
2. C
3. b
4. E
5. C
6. C
7. C
8. C
9. C
10. E
11. e
12. c
13. C
14. E
15. C
16. E
17. C
18. a
19. e
20. E
21. E
22. E
23. b
24. C
25. E
26. E
27. C
28. C
29. C
30. E
31. c
32. b
33. c
34. d
35. b
36. d
37. c
38. b
39. e
40. b
41. c
42. d
43. c
44. d
45. b
46. b
47. d
48. c
49. e
50. b
51. e
52. d
53. e
54. c
55. e
56. b

GABARITO COMENTADO

Questão 1 (CESPE/SEFAZ-RS/AUDITOR-FISCAL DA RECEITA ESTADUAL/BLOCO I/2019)

Julgue os itens a seguir, acerca de segurança da informação.

I – São exemplos de ameaças as contas sem senhas ou configurações erradas em serviços DNS, FTP e SMTP.

II – Não repúdio indica que o remetente de uma mensagem não deve ser capaz de negar que enviou a mensagem.

III – Vulnerabilidade é a fragilidade de um ativo ou de um grupo de ativos que pode ser explorada.

IV – Pessoas não são consideradas ativos de segurança da informação.

Estão certos apenas os itens

a) I e III.

b) I e IV.

c) II e III.

d) I, II e IV.

e) II, III e IV.

Letra c.

I – Errado. Ameaça (Ex.: vírus etc.) é algo que possa provocar danos à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio, mediante a exploração de uma determinada vulnerabilidade. São exemplos de vulnerabilidades as contas sem senhas ou configurações erradas em serviços DNS, FTP e SMTP.

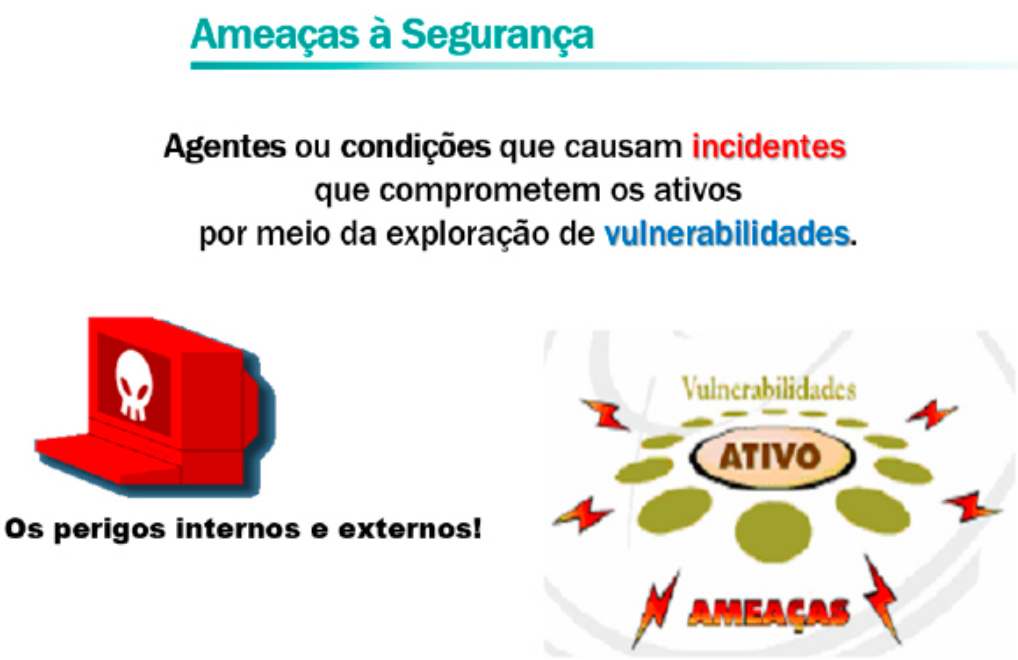


Figura – Ameaças à Segurança (QUINTÃO, 2016)

II – Certo. Não repúdio (ou irretratabilidade): indica que o emissor (aquele que assinou digitalmente a mensagem) não pode negar que foi o autor da mensagem, ou seja, não pode dizer mais tarde que a sua assinatura foi falsificada.

III – Certo. Vulnerabilidade é a fragilidade de um ativo ou de um grupo de ativos que pode ser explorada por uma ameaça para concretizar um ataque. Não há uma receita ou lista padrão de vulnerabilidades. Esta deve ser levantada junto a cada organização ou ambiente. Sempre se deve ter em mente o que precisa ser protegido e de quem precisa ser protegido de acordo com as ameaças existentes. Podemos citar, como exemplo inicial, uma análise de ambiente em uma sala de servidores de conectividade e Internet com a seguinte descrição: a sala dos servidores não possui controle de acesso físico. Eis a vulnerabilidade detectada nesse ambiente!

IV **– Errado.** Segundo Technet (2006) um ativo é "todo elemento que compõe o processo da comunicação, partindo da informação, seu emissor, o meio pelo qual é transmitida, até chegar ao seu receptor". Pessoas são consideradas ativos de segurança da informação. Aliás, são o elo mais fraco da segurança da informação!

Questão 2 (CESPE/PRF/2019) No acesso a uma página web que contenha o código de um vírus de script pode ocorrer a execução automática desse vírus, conforme as configurações do navegador.

Certo.

Vírus de scripts propagam-se por meio de scripts[1]. Dois tipos de scripts muito usados são os projetados com as linguagens Javascript (JS) e Visual Basic Script (VBS). Tanto um quanto o outro podem ser inseridos em páginas Web e interpretados por navegadores como Internet Explorer e outros. Assim, em virtude de ser interpretado pelo navegador Web, o vírus de scripts pode ser executado automaticamente pelo próprio navegador, dependendo de suas configurações.

Questão 3 (CESPE/SEFAZ-RS/AUDITOR-FISCAL DA RECEITA ESTADUAL/BLOCO I/2019) Para o estabelecimento de padrões de segurança, um dos princípios críticos é a necessidade de se verificar a legitimidade de uma comunicação, de uma transação ou de um acesso a algum serviço. Esse princípio refere-se à

a) confidencialidade.
b) autenticidade.
c) integridade.
d) conformidade.
e) disponibilidade.

Letra b.

Autenticidade é a propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo. Refere-se à **atribuição apropriada do proprietário ou criador dos dados.**

---

[1] **Scripts**: nome que designa uma sequência de comandos previamente estabelecidos e que são executados automaticamente em um sistema, sem necessidade de intervenção do usuário.

Questão 4 (CESPE/BNB/ANALISTA BANCÁRIO/2018) Acerca de pesquisas na Web e de vírus e ataques a computadores, julgue o item subsequente.

Entre as categorias de antivírus disponíveis gratuitamente, a mais confiável e eficiente é o scareware, pois os antivírus dessa categoria fazem uma varredura nos arquivos e são capazes de remover 99% dos vírus existentes.

Errado.

Scareware (também conhecido como software de engano, software de verificação desonesto ou fraudware) não é antivírus! Segundo Kaspersky Lab, trata-se de um software malicioso que faz com que os usuários de computadores acessem sites infestados por malware.

O scareware pode vir na forma de caixas suspensas, que aparecem como avisos legítimos de empresas de software antivírus, alegando que os arquivos de seu computador foram infectados. São tão habilmente criados que os usuários ficam assustados e pagam uma taxa para adquirir rapidamente um software que irá resolver o suposto problema. Mas o que eles acabam baixando é um falso software antivírus que na verdade é um malware destinado a roubar os dados pessoais da vítima.

Questão 5 (CESPE/BNB/ANALISTA BANCÁRIO/2018) Acerca de pesquisas na Web e de vírus e ataques a computadores, julgue o item subsequente.

Se um rootkit for removido de um sistema operacional, esse sistema não voltará à sua condição original, pois as mudanças nele implementadas pelo rootkit permanecerão ativas.

Certo.

Rootkit é um tipo de malware cuja principal intenção é se camuflar, para assegurar a sua presença no computador comprometido, impedindo que seu código seja encontrado por qualquer antivírus. Isto é possível porque esta aplicação tem a capacidade de interceptar as solicitações feitas ao sistema operacional, podendo alterar o seu resultado.

O invasor, após instalar o rootkit, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

Assim, como poderá esconder processos, instalar outros programas, a retirada dessa ameaça não irá desfazer as mudanças já feitas!

Questão 6 (CESPE/POLÍCIA FEDERAL/PAPILOSCOPISTA POLICIAL FEDERAL/2018) No que se refere à segurança de computadores, julgue o item subsecutivo. Cavalos de Troia são exemplos de vírus contidos em programas aparentemente inofensivos e sua ação danosa é mascarada pelas funcionalidades do hospedeiro.

Certo.

Questão MUITO POLÊMICA! Foi alvo de inúmeros recursos, mas o gabarito final foi considerado correto pela banca.

Cavalo de troia, trojan ou trojan-horse, é um 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.

Exemplos de trojans são programas que você recebe ou obtém de sites na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

O cavalo de troia pode carregar dentro de si vírus e outros códigos maliciosos, no entanto, ele não é um vírus! A classificação mais adequada para malware é a que foi explicitada em https://cartilha.cert.br/malware/.

Questão 7 (CESPE/POLÍCIA FEDERAL/AGENTE DA POLÍCIA FEDERAL/2018) Julgue o próximo item, a respeito de proteção e segurança, e noções de vírus, worms e pragas virtuais. A infecção de um sistema por códigos maliciosos pode ocorrer por meio da execução de arquivos infectados obtidos de anexos de mensagens eletrônicas, de mídias removíveis, de páginas web comprometidas, de redes sociais ou diretamente de outros equipamentos.

Certo.

A infecção de um sistema por códigos maliciosos pode ocorrer:

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pela autoexecução de mídias removíveis infectadas, como pen-drives;

- pelo acesso a páginas Web maliciosas, utilizando navegadores vulneráveis;
- pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Questão 8 (CESPE/POLÍCIA FEDERAL/ESCRIVÃO DE POLÍCIA FEDERAL/2018) Acerca de redes de computadores e segurança, julgue o item que segue.

Os aplicativos de antivírus com escaneamento de segunda geração utilizam técnicas heurísticas para identificar códigos maliciosos.

Certo.

Quanto ao método de detecção, os antivírus geralmente utilizam:

- Assinatura: uma lista de assinaturas é usada à procura de padrões;
- Heurística: baseia-se nas estruturas, instruções e características que o código malicioso possui; e
- Comportamento: baseia-se no comportamento apresentado pelo código malicioso quando executado.

Os aplicativos de antivírus com escaneamento de segunda geração utilizam técnicas heurísticas para identificar códigos maliciosos.

Questão 9 (CESPE/PC-MA/2018) Julgue o item subsequente, relativo a software para o ambiente de microinformática e a proteção e segurança da informação.

Fazer becape regularmente é uma conduta que permite minimizar os danos decorrentes de um ataque do tipo ransomware locker, que impede o acesso ao equipamento infectado, visto que o pagamento do resgate não garante acesso aos dados.

Certo.

Para se proteger de ransomware você deve tomar os mesmos cuidados que toma para evitar os outros códigos maliciosos, como ter um antivírus instalado e ser cuidadoso ao clicar em links ou abrir arquivos. Fazer backups regularmente também é essencial para proteger os seus dados pois, se seu equipamento for infectado, a única solução realmente efetiva para acessá-los novamente é buscá-los em seus backups.

Questão 10 (CESPE/PM-MA/2018) A seguir são apresentadas três situações hipotéticas.

I – Um usuário, após sequestro de seus dados, recebeu a informação de que, para reavê-los, seria necessário realizar um pagamento ao sequestrador.

II – Um usuário recebeu informação, por meio do setor de segurança da informação do seu órgão, de que seu computador, sem seu conhecimento, havia sido usado em um ataque a uma rede de outro órgão.

III – Em um dado momento do dia, um usuário notou que sua máquina estava consumindo mais recursos de memória do que o habitual e, ao executar no computador um programa de proteção, obteve a seguinte mensagem: “arquivo xpto infectado com o worm xyz”.

Com referência a essas situações hipotéticas e à segurança da informação, julgue o item subsequente.

A situação III caracteriza-se mais como vírus do que como um worm, pois os vírus são responsáveis por consumir muitos recursos, ao passo que os worms permitem o retorno de um invasor ao computador comprometido.

Errado.

O backdoor (porta dos fundos) é um programa que, colocado no micro da vítima, cria uma ou mais falhas de segurança, para permitir que o invasor que o colocou possa facilmente “voltar” àquele computador em um momento seguinte.

Worms são programas parecidos com vírus, mas que na verdade são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador (observe que os worms apenas se copiam, não infectam outros arquivos, eles mesmos são os arquivos!).

Diferentemente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores. Os worms são responsáveis por consumir muitos recursos, ao passo que os backdoors permitem o retorno de um invasor ao computador comprometido. Assim, conforme visto, a banca trocou a definição de worms pela de backdoors nessa assertiva.

Questão 11 (CESPE/TCE-PB/2018) Entre os vários tipos de programas utilizados para realizar ataques a computadores, aquele capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo entre computadores, é conhecido como

a) botnet.
b) spyware.
c) backdoor.
d) trojan.
e) worm.

Letra e.

O **Worm** ("verme" autorreplicante) é um tipo de praga virtual (malware) que se propaga automaticamente pelas redes de computadores, explorando vulnerabilidades existentes nessas redes ou falhas na configuração de softwares instalados nos computadores dessas redes e enviando cópias de si mesmo de computador para computador.

Após realizado o envio da cópia, o worm necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:

- imediatamente após ter sido transmitido, pela exploração automática de vulnerabilidades em programas sendo executados no computador alvo no momento do recebimento da cópia. Observe que nesse caso, não é necessária uma ação do usuário;
- diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu computador; pela realização de uma ação específica do usuário, a qual o worm está condicionado como, por exemplo, a inserção de uma mídia removível.

Questão 12 (CESPE/PC-MA/ESCRIVÃO DE POLÍCIA/2018) Determinado tipo de vírus eletrônico é ativado quando um documento por ele infectado é aberto, podendo então, nesse momento, infectar não apenas outros documentos, mas também um gabarito padrão de documento, de modo que cada novo documento criado sob esse gabarito seja infectado. Tal vírus, cuja propagação ocorre quando documentos por ele infectados são remetidos por correio eletrônico para outros usuários, é conhecido como

a) vírus de setor de carga (boot sector).

b) vírus de programa.

c) vírus de macro.

d) backdoor.

e) hoax.

Letra c.

a) **Errada. Vírus de Setor de Carga (Boot Setor) ou Vírus de Boot** infecta o setor de boot (ou MBR – Master Boot Record – Registro Mestre de Inicialização) dos discos rígidos.

> **Obs.:** o Setor de Boot do disco rígido é a primeira parte do disco rígido que é lida quando o computador é ligado. Essa área é lida pelo BIOS (programa responsável por "acordar" o computador) a fim de que seja encontrado o Sistema Operacional (o programa que vai controlar o computador durante seu uso).

b) **Errada.** Infectam arquivos de programa (de inúmeras extensões, como.exe,.com,.vbs,.pif).

c) **Certa** Um vírus de macro é parte de um arquivo normalmente manipulado por algum aplicativo que utiliza macros e que, para ser executado, necessita que o arquivo que o contém esteja aberto para que ele execute uma série de comandos automaticamente e infecte outros arquivos no computador (Cespe/2010).

Macro: conjunto de comandos que são armazenados em alguns aplicativos e utilizados para automatizar tarefas repetitivas.

Existem alguns aplicativos que possuem arquivos base (modelos - gabarito padrão de documentos) que são abertos sempre que o aplicativo é executado. Caso este arquivo base seja infectado pelo vírus de macro, toda vez que o aplicativo for executado, o vírus também será. Arquivos nos formatos gerados por programas da Microsoft, como o Word, Excel, Powerpoint e Access são os mais suscetíveis a este tipo de vírus. Arquivos nos formatos RTF, PDF e PostScript são menos suscetíveis, mas isso não significa que não possam conter vírus.

Normal.dot–Principal alvo de vírus de macro p/Word

d) Errada. O backdoor (porta dos fundos) é um programa que, colocado no micro da vítima, cria uma ou mais falhas de segurança, para permitir que o invasor que o colocou possa facilmente "voltar" àquele computador em um momento seguinte.

e) Errada. Hoaxes (boatos) são as histórias falsas recebidas por e-mail, sites de relacionamentos e na Internet em geral, cujo conteúdo, além das conhecidas correntes, consiste em apelos dramáticos de cunho sentimental ou religioso, supostas campanhas filantrópicas, humanitárias ou de socorro pessoal ou, ainda, falsos vírus que ameaçam destruir, contaminar ou formatar o disco rígido do computador.

Questão 13 (CESPE/ANVISA/2016) Códigos maliciosos podem ter acesso aos dados armazenados no computador e executar ações em nome dos usuários, de acordo com as permissões de operação de cada um destes.

Certo.

Os códigos maliciosos são programados com o intuito de prejudicar os sistemas de informação, alterar o funcionamento de programas, roubar informações do usuário da máquina, dentre outros. Esses códigos podem obter acesso aos dados que estão armazenados em um computador, e executar ações se passando por um determinado usuário, de acordo com os privilégios que o usuário tiver no sistema.

Geralmente, há três tipos de contas que podem ser utilizadas no computador, sendo que cada tipo oferece aos usuários um nível diferenciado de controle da máquina:

- a conta de **administrador**, com total privilégio sobre a máquina, fornece mais controle do computador e deve ser usada quando necessário;
- a conta **padrão**, sem privilégios administrativos, é a que deve ser usada para o dia a dia;
- a conta de **convidado**, também sem privilégios administrativos, destina-se às pessoas que precisam usar temporariamente o computador.

Portanto, se um usuário que é um administrador da máquina e possui privilégios administrativos completos sobre o equipamento teve a máquina contaminada por um código malicioso, essa ameaça poderá executar quaisquer ações nesse sistema, colocando em risco a segurança do computador.

Questão 14 (CESPE/DPU/ANALISTA/2016) A respeito da Internet e suas ferramentas, julgue o item a seguir.

Malwares são mecanismos utilizados para evitar que técnicas invasivas, como phishing e spams, sejam instaladas nas máquinas de usuários da Internet.

Errado.

Spams são mensagens de correio eletrônico não autorizadas ou não solicitadas pelo destinatário, geralmente de conotação publicitária ou obscena.

Phishing (ou scam) não é um programa que pode ser instalado no computador do usuário, mas sim um nome dado a um tipo de golpe eletrônico que tem o objetivo de "pescar" (roubar) informações e dados pessoais importantes (como senhas, dados bancários etc.) da vítima através da criação de um website falso e/ou do envio de uma mensagem eletrônica falsa.

Malwares (combinação de malicious software – programa malicioso) são softwares maliciosos, programados com o intuito de prejudicar os sistemas de informação, alterar o funcionamento de programas, roubar informações, causar lentidões de redes computacionais, dentre outros. Em outras palavras, malwares são programas que executam deliberadamente ações mal-intencionadas em um computador, comprometendo a segurança da informação, ao contrário do que foi reportado na questão!

Questão 15 (CESPE/INSS/TÉCNICO DO INSS/2016) A infecção de um computador por vírus enviado via correio eletrônico pode se dar quando se abre arquivo infectado que porventura esteja anexado à mensagem eletrônica recebida.

Certo.

Isso mesmo! Se o usuário fizer a abertura de um arquivo com vírus, a execução do arquivo infectado aciona o vírus, causando a infecção do computador.

É interessante manter, em seu computador:

- um antivírus funcionando constantemente (preventivamente);
- esse programa antivírus verificando os e-mails constantemente (preventivo);
- o recurso de atualizações automáticas das definições de vírus habilitado;
- as definições de vírus atualizadas constantemente (nem que para isso seja necessário, todos os dias, executar a atualização manualmente).

Questão 16 (CESPE/INSS/ANALISTA DO SEGURO SOCIAL COM FORMAÇÃO EM SERVIÇO SOCIAL/2016) Cada um dos próximos itens, que abordam procedimentos de informática e conceitos de Internet e intranet, apresenta uma situação hipotética, seguida de uma assertiva a ser julgada.

Ao iniciar seu dia de trabalho, Daniel se deparou com inúmeros aplicativos abertos em seu computador de trabalho, o que deixava sua máquina lenta e sujeita a travamentos frequentes. Ele constatou, ainda, que somente um desses aplicativos era necessário para a execução de suas atividades.

Nessa situação, para melhorar o desempenho do seu computador, Daniel deve utilizar um aplicativo de antivírus instalado localmente, para eliminar os aplicativos que estiverem consumindo recursos além do normal.

Errado.

O antivírus não será utilizado para eliminar os aplicativos que estão consumindo recursos além do normal. Uma ação possível para eliminar esses aplicativos seria fechar os demais aplicativos que não são de interesse do usuário.

Questão 17 (CESPE/DPU/ANALISTA/2016) A respeito da Internet e suas ferramentas, julgue o item a seguir.

Integridade, confidencialidade e disponibilidade da informação, conceitos fundamentais de segurança da informação, são adotados na prática, nos ambientes tecnológicos, a partir de um conjunto de tecnologias como, por exemplo, criptografia, autenticação de usuários e equipamentos redundantes.

Certo.

A **C**onfidencialidade, a **I**ntegridade e a **D**isponibilidade são três conceitos fundamentais de segurança da informação.

Eles formam aquilo que chamamos de pirâmide ou tríade da Segurança da Informação (É possível encontrar a sigla **CID**, para fazer menção às iniciais desses 3 princípios!).

Princípio	Característica	Dica Complementar
Confidencialidade (ou sigilo)	É a garantia de que a informação não será conhecida por quem não deve. O acesso às informações deve ser limitado, ou seja, somente as pessoas explicitamente autorizadas podem acessá-las.	Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento.
Integridade	É a garantia de que a informação que foi armazenada é a que será recuperada. A integridade busca proteção contra codificação não autorizada. Modificação deve ser realizada somente pelas partes devidamente autorizadas.	A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.
Disponibilidade	Busca acesso disponível às entidades autorizadas sempre que necessário.	Manter a disponibilidade pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.

Esses princípios são aplicados na prática, nos ambientes tecnológicos, a partir de um conjunto de controles como, por exemplo, criptografia, autenticação de usuários e equipamentos redundantes (um sistema redundante possui um segundo dispositivo que está imediatamente disponível para uso quando da falha do dispositivo principal).

Aspecto	Descrição	Medidas de Controle
Confidencialidade	Garantia que a informação não será conhecida por quem não deve	Classificação da informação, criptografia.
Integridade	Garantia que a informação que foi armazenada é a que será recuperada	Autenticação de usuários e implementação de controle de acesso.
Disponibilidade	Garantia que a informação sempre poderá ser acessada	Plano de contingência Uso de equipamentos redundantes, etc.

Questão 18 (CESPE/TRE-PI/CONHECIMENTOS GERAIS PARA OS CARGOS 1, 2 E 4/2016)

A remoção de códigos maliciosos de um computador pode ser feita por meio de

a) anti-spyware.

b) detecção de intrusão.

c) anti-spam.

d) anti-phishing.

e) filtro de aplicações.

Letra a.

a) Certa. A ferramenta anti-spyware é uma forte aliada do antivírus, permitindo a localização e bloqueio de códigos maliciosos do tipo spywares. Exemplo de ferramentas anti-spyware: Windows Defender, Spybot etc.

Nem toda ferramenta anti-spyware é necessariamente antivírus e vice-versa. Há programas que apresentam as duas funções, mas isso nem sempre acontece!

b) Errada. Para detecção de intrusão o IDS (Intrusion Detection Systems – Sistemas de Detecção de Intrusos) é a ferramenta utilizada. IDS são sistemas de detecção de intrusos, que têm por finalidade detectar atividades incorretas, maliciosas ou anômalas, em tempo real, permitindo que algumas ações sejam tomadas. O IDS procura por ataques já catalogados e registrados, podendo, em alguns casos, fazer análise comportamental do sistema.

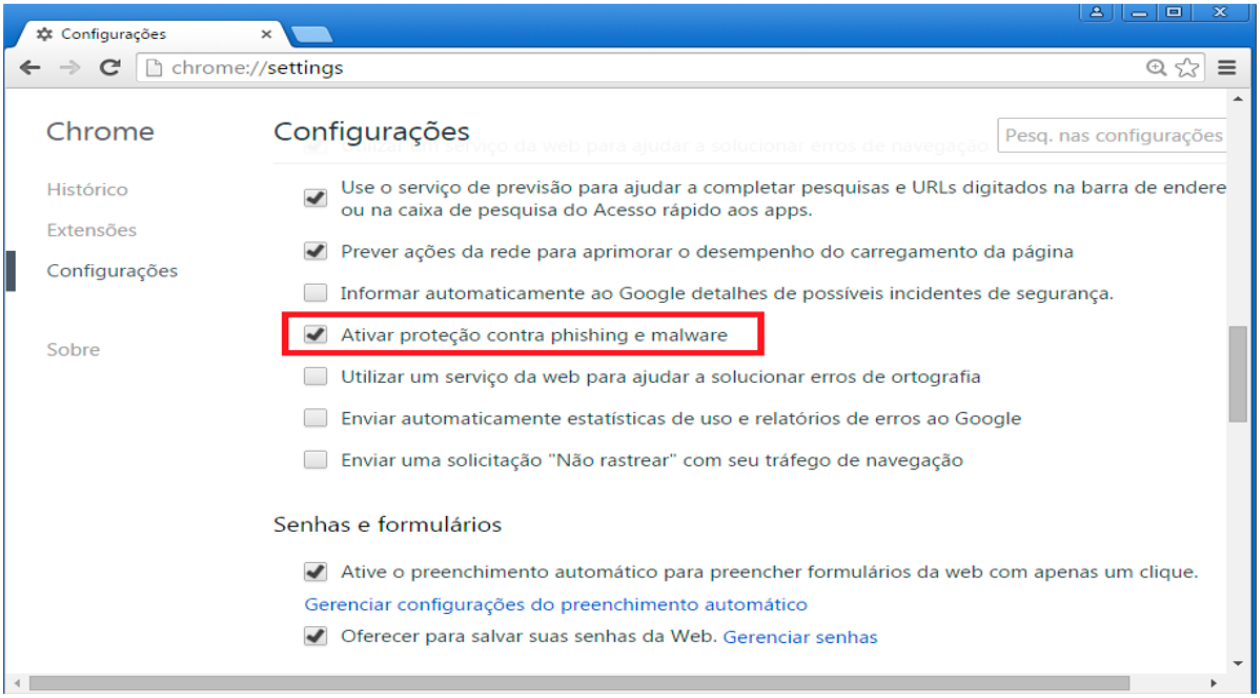
Geram logs para casos de tentativas de ataques e para casos em que um ataque teve sucesso. Assim como os firewalls, os IDSs também podem gerar falsos positivos (Uma situação em que o firewall ou IDS aponta uma atividade como sendo um ataque, quando na verdade não é).

Um IPS (Intrusion Prevention System - Sistema de Prevenção de Intrusos) é um sistema que detecta e obstrui automaticamente ataques computacionais a recursos protegidos. Diferente dos IDS tradicionais, que localizam e notificam os administradores sobre anomalias, um IPS defende o alvo SEM uma participação direta humana.

c) Errada. Anti-spam: ferramenta utilizada para filtro de mensagens indesejadas.

d) Errada. Phishing ou scam: não é um programa que pode ser instalado no computador do usuário, mas sim um nome dado a um tipo de golpe eletrônico que tem o objetivo de "pescar" (roubar) informações e dados pessoais importantes (como senhas, dados bancários etc.) da vítima através da criação de um website falso e/ou do envio de uma mensagem eletrônica falsa.

Para não ser vítima desse tipo de golpe, o usuário precisa estar muito atento e prevenido, e ferramentas anti-phishing gratuitas ou pagas, como Internet Explorer, Chrome etc. podem ser utilizadas. No entanto, essa proteção não irá fazer a remoção de códigos maliciosos do computador do usuário. Veja a seguir a caixa de seleção que pode ser ativada no Google Chrome para ativação da proteção contra phishing e malware.



e) Errada. Filtro de aplicações possibilita conhecer aplicações e seus comportamentos, estabelecendo bloqueios quando não estiverem em conformidade com a Política de Segurança da organização.

Questão 19 (CESPE/TRE-RS/TÉCNICO JUDICIÁRIO/CONHECIMENTOS BÁSICOS PARA OS CARGOS 6 A 8/2015) Em relação a vírus, worms e pragas virtuais, assinale a opção correta.

a) Para garantir a segurança da informação, é suficiente instalar e manter atualizados antivírus.

b) Não há diferença — seja conceitual, seja prática — entre worms e vírus; ambos são arquivos maliciosos que utilizam a mesma forma para infectar outros computadores.

c) Rootkits é um arquivo que infecta o computador sem causar maiores danos, ainda que implique a pichação da tela inicial do navegador.

d) A segurança da informação em uma organização depende integralmente de a sua área de tecnologia optar pela adoção de recursos de segurança atualizados, como firewall e antivírus.

e) Em segurança da informação, denominam-se engenharia social as práticas utilizadas para obter acesso a informações importantes ou sigilosas sem necessariamente utilizar falhas no software, mas, sim, mediante ações para ludibriar ou explorar a confiança das pessoas.

Letra e.

a) Errada. O antivírus é uma das ferramentas de segurança que devem ser implementadas para resguardar a segurança dos ativos (o que tem valor para o indivíduo ou organização e que merece ser protegido). Outras práticas de segurança também são recomendadas, como: conscientização de usuários, utilização de firewall etc.

b) Errada. Worms são programas parecidos com vírus, mas que na verdade são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador (observe que os worms apenas se copiam, não infectam outros arquivos, eles mesmos são os arquivos!).

Veja as principais diferenças entre essas ameaças na tabela seguinte:

VÍRUS	WORM
É um programa (ou parte de um programa) que se anexa a um arquivo de programa qualquer.	Programa.
Propaga-se inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.	Não embute cópias de si mesmo em outros programas ou arquivos. Propaga-se automaticamente pelas redes, enviando copias de si mesmo de computador para computador.
Depende da execução do programa ou arquivo hospedeiro para ser ativado.	Não necessita ser explicitamente executado para se propagar. Basta que se tenha execução direta de suas cópias ou a exploração automática de vulnerabilidades existentes em programas instalados em computadores.

c) Errada. Rootkit é um tipo de malware cuja principal intenção é se camuflar, para assegurar a sua presença no computador comprometido, impedindo que seu código seja encontrado por qualquer antivírus. Isto é possível porque esta aplicação tem a capacidade de interceptar as solicitações feitas ao sistema operacional, podendo alterar o seu resultado.

O invasor, após instalar o rootkit, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

Um rootkit pode fornecer programas com as mais diversas funcionalidades. Dentre eles, merecem destaque:

- programas para esconder atividades e informações deixadas pelo invasor, tais como arquivos, diretórios, processos etc.;
- backdoors, para assegurar o acesso futuro do invasor ao computador comprometido;
- programas para remoção de evidências em arquivos de logs;
- sniffers, para capturar informações na rede onde o computador está localizado, como por exemplo senhas que estejam trafegando em claro, ou seja, sem qualquer método de criptografia;
- scanners, para mapear potenciais vulnerabilidades em outros computadores.

Rootkit é um tipo de praga virtual de difícil detecção, visto que é ativado antes que o sistema operacional tenha sido completamente inicializado (CESPE/2013/PCDF).

d) Errada. Todas as áreas da organização devem estar envolvidas! Não adianta ter a melhor tecnologia se as pessoas não estão envolvidas com a temática de segurança e não colocam em ação no seu dia a dia as boas práticas de segurança.

e) Certa. Engenharia Social é a técnica de ataque utilizada para se obter informações sigilosas ou importantes de empresas e sistemas, enganando e explorando a confiança dos usuários.

Questão 20 (CESPE/TELEBRAS/ANALISTA SUPERIOR/COMERCIAL/2015) A respeito de segurança da informação, julgue o item subsecutivo.

Worms, assim como os vírus, são autorreplicáveis e necessitam ser executados pelos usuários para se propagarem e infectarem os computadores de uma rede.

Errado.

Worms são programas parecidos com vírus, mas que na verdade são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador (observe que os worms apenas se copiam, não infectam outros arquivos, eles mesmos são os arquivos!). Diferentemente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

Questão 21 (CESPE/TCE-RN/CONHECIMENTOS BÁSICOS PARA OS CARGOS 2 E 3/2015) Julgue o item subsequente, a respeito de organização e gerenciamento de arquivos, pastas e programas, bem como de segurança da informação.

A principal diferença entre crackers e hackers refere-se ao modo como esses malfeitores da área de segurança da informação atacam: os crackers são mais experientes e realizam ataques sem utilizar softwares, ao passo que os hackers utilizam códigos maliciosos associados aos softwares para realizar ataques ao ciberespaço.

Errado.

Os hackers, por sua definição geral, são aqueles que utilizam seus conhecimentos para invadir sistemas, não com o intuito de causar danos às vítimas, mas sim como um desafio às suas habilidades. Eles invadem os sistemas, capturam ou modificam arquivos para provar sua capacidade e depois compartilham suas proezas com os colegas. Não têm a intenção de prejudicar, mas sim de apenas demonstrar que conhecimento é poder.

Os crackers são elementos que invadem sistemas para roubar informações e causar danos às vítimas. O termo crackers também é uma denominação utilizada para aqueles que decifram códigos e destroem proteções de software.

Atualmente, a imprensa mundial atribui qualquer incidente de segurança a hackers, em seu sentido genérico. A palavra cracker não é vista nas reportagens, a não ser como cracker de senhas, que é um software utilizado para descobrir senhas ou decifrar mensagens cifradas.

Assim, não existe a diferença reportada na questão!

Para a prova, guarde o seguinte:

- **Hackers ("Do bem"):** invadem sistemas no intuito de demonstrar as suas habilidades e as vulnerabilidades do seu alvo.
- **Crackers ("Do mal"):** invadem sistemas com a finalidade de obter vantagem/dinheiro. Lembre-se da droga Crack para memorizar que Cracker é ruim, do mal! #FicaaDica

---

Questão 22 (CESPE/TJ-DFT/ANALISTA JUDICIÁRIO/CONHECIMENTOS BÁSICOS PARA OS CARGOS 2, 3 E 5 A 12/2015) Com relação a redes de computadores, Internet e respectivas ferramentas e tecnologias, julgue o item a seguir.

Na segurança da informação, controles físicos são soluções implementadas nos sistemas operacionais em uso nos computadores para garantir, além da disponibilidade das informações, a integridade e a confidencialidade destas.

Errado.

Controles físicos visam proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. Devem se basear em perímetros predefinidos nas imediações dos recursos computacionais, podendo ser explícitos como uma sala, cofre etc. ou implícitos, como áreas de acesso restrito.

Controles lógicos compreendem inúmeros procedimentos, adotados pela empresa ou intrínsecos aos sistemas utilizados, cujo objetivo é proteger os dados, programas e sistemas contra tentativas de acessos não autorizados, feitas por usuários ou outros programas.
Assim, as soluções implementadas nos sistemas operacionais estão relacionadas aos controles lógicos.

Questão 23 (CESPE/TRE-MT/TÉCNICO JUDICIÁRIO/ CONHECIMENTOS GERAIS PARA O CARGO 6/2015) A função principal de uma ferramenta de segurança do tipo antivírus é

a) monitorar o tráfego da rede e identificar possíveis ataques de invasão.
b) verificar arquivos que contenham códigos maliciosos.
c) fazer becape de segurança dos arquivos considerados críticos para o funcionamento do computador.
d) bloquear sítios de propagandas na Internet.
e) evitar o recebimento de mensagens indesejadas de e-mail, tais como mensagens do tipo spams.

Letra b.

Malwares (combinação de malicious software – programa malicioso) são softwares maliciosos, programados com o intuito de prejudicar os sistemas de informação, alterar o funcionamento de programas, roubar informações, causar lentidões de redes computacionais, dentre outros. A principal função de uma ferramenta de antivírus é verificar arquivos quanto à presença de códigos maliciosos (malware).

Questão 24 (CESPE/TJ-DFT/ANALISTA JUDICIÁRIO/CONHECIMENTOS BÁSICOS PARA OS CARGOS 2, 3 E 5 A 12/2015) A respeito de sistemas operacionais e aplicativos para edição de texto, julgue o item que se segue. Vírus do tipo boot, quando instalado na máquina do usuário, impede que o sistema operacional seja executado corretamente.

Certo.

Vírus de boot é um tipo de ameaça que infecta o setor de boot (ou MBR – Master Boot Record – Registro Mestre de Inicialização) dos discos rígidos. Com o vírus de boot, por afetar os arquivos de inicialização, o funcionamento do sistema operacional é prejudicado. O sistema operacional já será iniciado infectado e sistematicamente não funcionará corretamente.

Questão 25 (CESPE/TELEBRAS/ANALISTA ADMINISTRADOR/ CONHECIMENTOS BÁSICOS PARA O CARGO 3/2015) No que se refere à segurança da informação, julgue o seguinte item.

Sniffers são programas aparentemente inofensivos cuja principal característica é utilizar a técnica de mascaramento. A técnica em questão permite, por exemplo, que um sniffer seja anexado a um jogo, que, por sua vez, ao ser instalado em um computador, coletará informações bancárias do usuário.

Errado.

Cavalo de Troia (ou Trojan Horse) é um programa, normalmente recebido como um "presente" (por exemplo cartão virtual, álbum de fotos, protetor de tela, jogo etc.), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário. Assim, esse programa aparentemente inofensivo, que utiliza a técnica de mascaramento, é o cavalo de troia.

Um sniffer atua na rede farejando pacotes na tentativa de encontrar certas informações (trata-se de um malware quando fareja pacotes da rede em busca de informações não autorizadas, como nomes de usuários, senhas ou qualquer outra informação transmitida que não esteja criptografada).

Questão 26 (CESPE/TELEBRAS/ANALISTA SUPERIOR/COMERCIAL/2015) A respeito de segurança da informação, julgue o item subsecutivo.

Uma das formas de manter o aparelho de telefone celular livre de vírus é deixar o bluetooth habilitado constantemente, para que ele possa identificar possíveis anexos maliciosos às mensagens recebidas.

Errado.

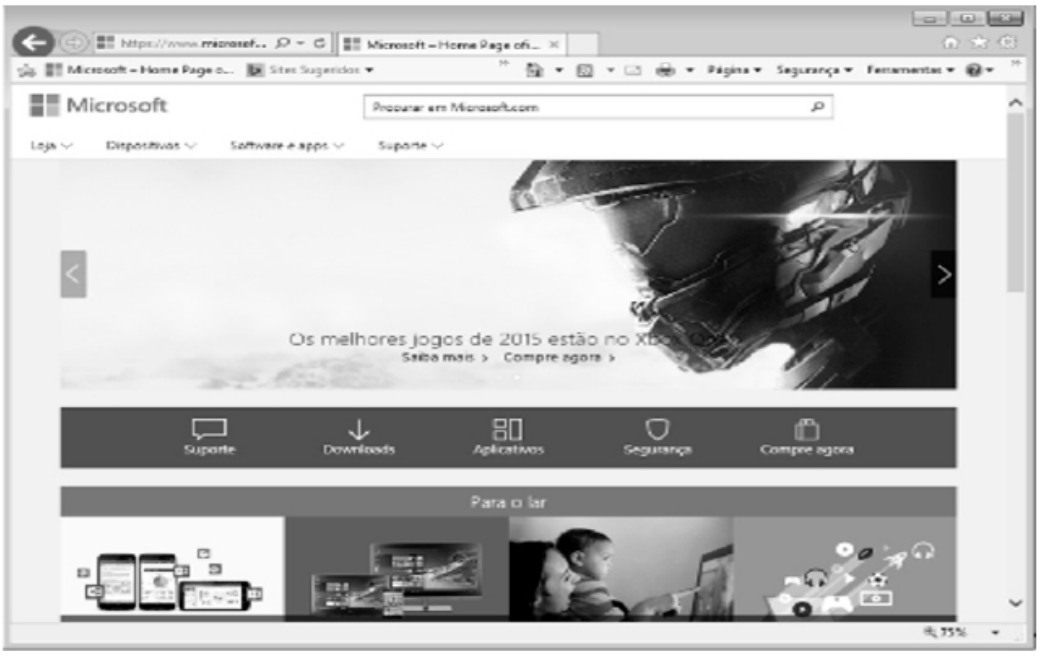
A utilização do bluetooth (ativada durante todo o tempo) irá contribuir para disseminar códigos maliciosos (vírus de celular, worms etc.) no aparelho de telefone celular reportado na questão, possibilitando a invasão por terceiros naquele dispositivo.

Depois de infectar um telefone celular, o vírus de celular pode realizar diversas atividades, tais como:

- destruir/sobrescrever arquivos;
- remover contatos da agenda;
- efetuar ligações telefônicas;
- o aparelho fica desconfigurado e tentando se conectar via Bluetooth com outros celulares;
- a bateria do celular dura menos do que o previsto pelo fabricante, mesmo quando você não fica horas pendurado nele;
- emitir algumas mensagens multimídia esquisitas;
- tentar se propagar para outros telefones.

A ativação do bluetooth não tem relação com a identificação de possíveis anexos maliciosos nas mensagens recebidas.

Questão 27 (CESPE/CEBRASPE/MP-ENAP/ADMINISTRADOR CARGO 1/2015)



A respeito da figura acima apresentada, do Internet Explorer 11 e de segurança da informação, julgue o item a seguir.

Trackwares são programas que rastreiam a atividade do sistema, reúnem informações do sistema ou rastreiam os hábitos do usuário, retransmitindo essas informações a organizações de terceiros.

Certo.

Conforme destaca Norton Security (2014),

> (...) **trackwares** são programas que rastreiam a atividade do sistema, reúnem informações do sistema ou rastreiam os hábitos do usuário, retransmitindo essas informações a organizações de terceiros.

As informações reunidas por esses programas não são confidenciais nem identificáveis. Os programas de trackware são instalados com o consentimento do usuário e também podem estar contidos em pacotes de outro software instalado pelo usuário.

Questão 28 (CESPE/TRE-GO/ANALISTA JUDICIÁRIO/2015) Acerca de procedimentos de segurança e de ensino a distância, julgue o item subsecutivo. [Botnet é uma rede formada por inúmeros computadores zumbis e que permite potencializar as ações danosas executadas pelos bots, os quais são programas similares ao worm e que possuem mecanismos de controle remoto].

Certo.

De modo similar ao worm, bot ("robô") é um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de software instalado em um computador. Adicionalmente ao worm, dispõe de mecanismos de comunicação com o invasor, permitindo que o bot seja controlado remotamente. Os bots esperam por comandos de um hacker, podendo manipular os sistemas infectados, sem o conhecimento do usuário.

Botnet (também conhecida como rede zumbi) é uma rede infectada por bots, sendo composta geralmente por milhares desses elementos maliciosos, que ficam residentes nas máquinas, aguardando o comando de um invasor. Quanto mais zumbis (Zombie Computers) participarem da botnet, mais potente ela será. Um invasor que tenha controle sobre uma botnet pode utilizá-la para:

- coletar informações de um grande número de computadores;
- "clicar" em anúncios e gerar receitas fraudulentas;
- enviar spam em grande escala;
- hospedar sites de phishing;
- iniciar ataques de negação de serviço que impedem o uso de serviços online etc.

Questão 29 (CESPE/TRE-GO/ANALISTA JUDICIÁRIO/2015) Acerca de procedimentos de segurança e de ensino a distância, julgue o item subsecutivo. Quanto à segurança da informação, sugere-se que se crie um disco de recuperação do sistema, assim como se desabilite a autoexecução de mídias removíveis e de arquivos anexados.

Certo.

Todas as atividades mencionadas na questão são boas práticas de segurança. Um disco de recuperação de sistema pode ser usado para reiniciar o computador. Ele também contém ferramentas que podem ajudá-lo a recuperar o sistema operacional do computador de erros sérios ou restaurar o computador usando uma imagem do sistema.

A desativação da autoexecução de mídias removíveis e de arquivos anexados é um dos itens para que se evite a contaminação por *malwares* (códigos maliciosos).

Questão 30 (CESPE/CADE/NÍVEL INTERMEDIÁRIO/NÍVEL MÉDIO/2014) Acerca dos conceitos de gerenciamento de arquivos e de segurança da informação, julgue o item subsequente. O computador utilizado pelo usuário que acessa salas de bate-papo não está vulnerável à infecção por worms, visto que esse tipo de ameaça não se propaga por meio de programas de chat.

Errado.

O malware (código malicioso) do tipo Worm pode infectar máquinas desprotegidas, a partir da utilização de programas de chat. A contaminação pode acontecer, por exemplo, através de textos e fotografias enviados através do programa de chat, com o auxílio de encurtadores de URL. Caso uma pessoa clique em um dos endereços falsos, a máquina é contaminada automaticamente pelo malware, que em seguida pode se espalhar pela rede de contatos do usuário.

Figura. Bate-Papo

Para prevenção contra worms, mantenha o sistema operacional e demais softwares do equipamento sempre atualizados; aplique todas as correções de segurança (patches) disponibilizadas pelos fabricantes, para corrigir eventuais vulnerabilidades existentes nos softwares utilizados; instale um firewall pessoal, que em alguns casos pode evitar que uma vulnerabilidade existente seja explorada **(observe que o firewall não corrige as vulnerabilidades!)** ou que um worm se propague.

Questão 31 (FCC/TRT-14ª REGIÃO/RO E AC/ANALISTA JUDICIÁRIO/ESTATÍSTICA/2018)

Crime cibernético é todo crime que é executado online e inclui, por exemplo, o roubo de informações no meio virtual. Uma recomendação correta de segurança aos usuários da internet, para se proteger contra a variedade de crimes cibernéticos é

a) usar a mesma senha (composta por letras maiúsculas e minúsculas, números e símbolos) em todos os sites com conteúdo de acesso restrito, mantendo esta senha protegida em um aplicativo de gerenciamento de senhas.

b) manter os softwares atualizados, exceto os sistemas operacionais, pois estes já possuem mecanismos de segurança como firewall, antivírus e antispyware.

c) gerenciar as configurações de mídias sociais para manter a maior parte das informações pessoais e privadas bloqueadas.

d) proteger a rede wireless com senha que utiliza criptografia Wired Equivalent Privacy – WEP ou com uma Virtual Protect Network – VPN.

e) usar uma suíte de segurança para a internet com serviços como firewall, blockwall e antivírus, como o LibreOffice Security Suit.

Letra c.

a) Errada. Alguns elementos que você deve usar na elaboração de suas senhas são: números aleatórios; grande quantidade de caracteres; diferentes tipos de caracteres (CERT.BR,2013). Mais dicas:

- crie uma senha que contenha pelo menos oito caracteres, compostos de letras, números e símbolos.

- utilize uma senha diferente para cada serviço (por exemplo, uma senha para o banco, outra para acesso à rede corporativa da sua empresa, outra para acesso a seu provedor de Internet etc.);
- altere a senha com frequência;
- crie tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador;
- utilize o usuário Administrator (ou root) somente quando for estritamente necessário.

b) Errada. É importante fazer a instalação de patches de segurança e atualizações corretivas de softwares e do sistema operacional quando forem disponibilizadas.

c) Certa. Tal cuidado é de grande valia, principalmente no que diz respeito à segurança pessoal. Publicar fotos com uniforme escolar, que sugerem ostentação e os locais que costuma frequentar pode ser um grande atrativo para ações criminosas, por exemplo.

d) Errada. WEP (Wired Equivalency Privacy - sigla de "Privacidade Equivalente à de Redes com Fios") foi a primeira tentativa de se criar um protocolo eficiente de proteção de redes WI-FI em 1997. Hoje é um protocolo obsoleto no quesito segurança. WPA (Wi-Fi Protected Access - sigla de "Acesso Protegido a Wi-Fi") é um subconjunto dos padrões 802.11i, e serviu como um padrão de "transição" entre o WEP e o WPA2. O WPA2 segue o padrão 802.11i e substitui formalmente o WEP. Assim, é mais seguro do que o WEP!

Uma VPN (Virtual Private Network – Rede Privada Virtual) é uma rede privada (não é de acesso público!) que usa a infraestrutura de uma rede pública já existente (como, por exemplo, a Internet) para transferir seus dados (os dados devem estar criptografados para passarem despercebidos e inacessíveis pela Internet).

As VPNs são muito utilizadas para interligar filiais de uma mesma empresa, ou fornecedores com seus clientes (em negócios eletrônicos), por meio da estrutura física de uma rede pública. O tráfego de dados é levado pela rede pública utilizando protocolos não necessariamente seguros.

e) Errado. LibreOffice Security Suit não é um produto existente no mercado.

Questão 32 (FCC/SEGEP-MA/2018) Em uma situação hipotética, um funcionário da Secretaria de Estado da Gestão e Assistência dos Servidores (SEGEP) verificou que um tipo de código malicioso (malware) havia invadido e tornado inacessíveis os dados armazenados em seu equipamento porque tudo havia sido criptografado. O invasor exigiu pagamento de resgate para restabelecer o acesso.

Essa situação mostra a ocorrência do ataque cibernético de um malware conhecido por:

a) Spam.

b) Ransomware.

c) Trojan Spy.

d) Cookie.

e) Worm.

Letra b.

Ransomware é um tipo de malware que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.

Existem dois tipos de ransomware:

Ransomware Locker: impede que você acesse o equipamento infectado.

Ransomware Crypto: impede que você acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia, para impedir que o usuário tenha acesso aos dados.

Para se proteger de ransomware você deve tomar os mesmos cuidados que toma para evitar os outros códigos maliciosos, como ter um antivírus instalado e ser cuidadoso ao clicar em links ou abrir arquivos. Fazer backups regularmente também é essencial para proteger os seus dados pois, se seu equipamento for infectado, a única solução realmente efetiva para acessá-los novamente é buscá-los em seus backups.

Como exemplo, a ameaça conhecida como Wannacry é um tipo de ransomware que atacou uma enorme quantidade de computadores em diversas partes do mundo em 2017 e conseguiu se infiltrar nesses equipamentos graças a uma vulnerabilidade no Windows.

Questão 33 (FCC/AGED–MA/2018) Não importa se um usuário utiliza Microsoft, MacOS, Android ou outro tipo de sistema operacional, pois ao se conectar na internet com um deles, já fica vulnerável a uma infinidade de ataques digitais e pode sofrer com um tipo de malware cuja invasão é realizada com o intuito de causar algum dano ou roubar informações.

(Adaptado de: http://tecnologia.ig.com.br/2017-04-04/malware-cimes-ciberneticos.html)

O malware referenciado no texto é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções maliciosas sem o conhecimento do usuário. Ataca através de programas que necessitam ser explicitamente executados para que sejam instalados, mas também pode ser instalado por atacantes que, após invadirem o computador, alteram programas já existentes para que também executem ações maliciosas. Este malware e denominado:

a) worm.

b) rootkit.

c) trojan.

d) wanna cry.

e) ransomware.

Letra c.

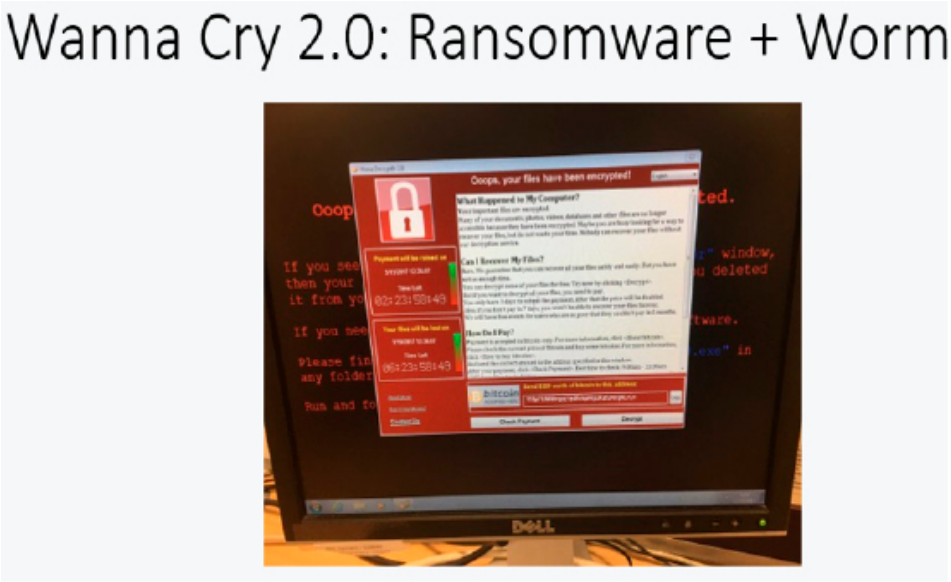
a) Errada. Worms são programas parecidos com vírus, mas que na verdade são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador (observe que os worms apenas se copiam, não infectam outros arquivos, eles mesmos são os arquivos!).

b) Errada. Rootkit é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. O conjunto de programas e técnicas fornecido pelos rootkits pode ser usado para: remover evidências em arquivos de logs; instalar outros códigos maliciosos, como backdoors, para assegurar o acesso futuro ao computador infectado; esconder atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões de rede, etc.; mapear potenciais vulnerabilidades em outros computadores, por meio de varreduras na rede; capturar informações da rede onde o computador comprometido está localizado, pela interceptação de tráfego (CertBr,2013).

c) Certa. Trojan Horse (Cavalo de Troia) é um programa aparentemente inofensivo que entra em seu computador na forma de cartão virtual, álbum de fotos, protetor de tela, jogo etc., e que, quando executado (com a sua autorização), parece lhe divertir, mas, por trás **possui funcionalidades maliciosas escondidas**, que permitem, por exemplo, abrir portas de comunicação do seu computador para que ele possa ser invadido ou monitorado etc.

> Por definição, o Cavalo de Troia distingue-se de um vírus ou de um worm por NÃO infectar outros arquivos, NEM propagar cópias de si mesmo automaticamente.

d) Errada. Conforme foi noticiado pela imprensa, um ataque cibernético de grandes proporções iniciou-se em 12/05/17, afetando diversas empresas ao redor do mundo. A ameaça principal detectada neste cenário é um ransomware, conhecido pelas variantes de WannaCry ou HydraCrypt, que infecta computadores utilizando o sistema operacional Microsoft Windows através de uma vulnerabilidade no serviço SMB, utilizado para o compartilhamento de arquivos via rede.



Resumindo, trata-se de uma infecção por malware do tipo “ransomware”, que se caracteriza por criptografar os arquivos dos usuários e exigir um “resgate” em dinheiro eletrônico, conhecido como Bitcoin (moeda virtual), para que seja fornecida a senha de recuperação desses dados. Além de ransomware, atua como um worm, propagando-se automaticamente pelas redes com máquinas desatualizadas (uma vez que um computador seja infectado, ele tentará propagar essa infecção para os demais computadores conectados na mesma rede).

e) Errada. Ransomware é um tipo de malware que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de **resgate** (ransom) para restabelecer o acesso ao usuário.

Questão 34 (FCC/ALESE/TÉCNICO LEGISLATIVO/TÉCNICO-ADMINISTRATIVO/2018) Uma ação que NÃO potencializa o risco de golpes (scam) na Internet e de infecção de computador por malware é

a) baixar atualizações ou softwares em sites de acesso mais rápido que o do fabricante.

b) entrar em sites para baixar uma faixa musical, álbum ou filmes sem pagar.

c) utilizar a mesma senha complexa em todos os sites que possui cadastro.

d) utilizar Virtual Private Network confiável para acessar a Internet em locais públicos.

e) abrir arquivos anexos no webmail, quando o assunto indicar alta prioridade.

Letra d.

A questão quer que listemos uma boa prática de segurança que pode ser utilizada no combate a golpes de Phishing (scam), evitando também infecção de computador por malware (códigos maliciosos). Nesse contexto a letra "d" é a resposta.

a) Errada. Seja cuidadoso ao acessar links para baixar atualizações ou softwares, e procure acessar o site do fabricante diretamente. Por exemplo, atualizações de segurança do Windows serão feitas a partir do site da Microsoft. Ao baixar atualizações ou softwares de sites desconhecidos o seu risco é alto!

b) Errada. Com essa ação você poderá contaminar o computador com produtos de origem desconhecida, piratas e com códigos maliciosos.

c) Errada. Senhas são utilizadas no processo de verificação da identidade do usuário (login), assegurando que este é realmente quem diz ser. Utilize uma senha diferente para cada sistema utilizado. Uma vez descoberta a sua senha, se ela for a mesma em todos os sites, todos os acessos a esses ambientes ficarão comprometidos.

d) Certa. Virtual Private Network (VPN) ou Rede Virtual Privada é uma rede privada (rede com acesso restrito) construída sobre a estrutura de uma rede pública, normalmente a Internet. Criam "túneis" virtuais de transmissão de dados utilizando criptografia, mais segura que a rede pública (internet).

e) Errada. Os anexos dos e-mails podem estar contaminados, mesmo em mensagens de alta prioridade.

Questão 35 (FCC/METRÔ-SP/OFICIAL LOGÍSTICA ALMOXARIFADO I/2018) O usuário de um computador deu um duplo clique sobre um programa recebido por e-mail, executando-o, e seu computador foi infectado por um malware que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e/ou arquivos. Tais características permitem concluir que o computador foi infectado por um

a) warm.
b) vírus.
c) rootkit.
d) botnet.
e) backdoor.

Letra b.

a) Errada. O termo correto da ameaça em A é Worm, e não Warm, como destacado pela banca. Worm é um programa capaz de se propagar **automaticamente** pelas redes, enviando cópias de si mesmo de computador para computador (observe que os worms apenas se copiam, não infectam outros arquivos, eles mesmos são os arquivos!).

b) Certa. O vírus, resposta da questão, é um 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/ou arquivos.

c) Errada. Rootkit é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso, sendo ativado antes que o sistema operacional esteja totalmente inicializado.

d) Errada. Botnet (Rede Zumbi) é uma rede infectada por bots, sendo composta geralmente por milhares desses elementos maliciosos, que ficam residentes nas máquinas, aguardando o comando de um invasor.

e) Errada. Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes que exploram vulnerabilidades existentes nos programas instalados para invadi-lo.

Questão 36 (FCC/SEGEP-MA/AUXILIAR DE FISCALIZAÇÃO AGROPECUÁRIA/2018) Ataques cibernéticos causaram prejuízo de US$ 280 bilhões às corporações

A extorsão virtual, quando servidores de empresas são bloqueados e seus gestores só recebem acesso novamente mediante pagamento para os criminosos, também é um dos maiores problemas na América Latina, 28,1%, ficando atrás apenas do bloco de países Asiáticos, 35,1%. Os setores mais suscetíveis a essa modalidade de ataques cibernéticos são serviços financeiros (45,8%); cuidados da saúde (23,7%); energia (23,3%); bens de consumo (22,4%); educação (22,1%); viagem, turismo e lazer (19,8%); agricultura (17,9%); setor produtivo (16,3%); tecnologia, meios de comunicação e telecomunicações (13,0%); transporte (11,3%); imobiliário e construção (6,2%) e serviços profissionais (4,8%).

(Disponível em: http://www.convergenciadigital.com.br)

O texto se refere à "extorsão virtual, quando servidores de empresas são bloqueados e seus gestores só recebem acesso novamente mediante pagamento para os criminosos" e quase 18% deste tipo de ataque atinge o setor de agricultura. A denominação deste tipo de ataque é

a) bot.

b) spyware.

c) backdoor.

d) ransomware.

e) rootkit.

Letra d.

a) Errada. Bots ("Robôs"), de modo similar ao worm, é um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de software instalado em um computador. Adicionalmente ao worm, dispõe de mecanismos de comunicação com o invasor, permitindo que o bot seja controlado remotamente. Os bots esperam por comandos de um hacker, podendo manipular os sistemas infectados, sem o conhecimento do usuário.

b) Errada. Spyware é um programa espião (spy em inglês = espião), que tem por finalidade monitorar as atividades de um sistema e enviar as informações coletadas para terceiros, sem o consentimento da parte envolvida.

c) Errada. Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

d) Certa. Ransomware é um tipo de malware que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de **resgate** (ransom) para restabelecer o acesso ao usuário.

e) Errada. Rootkit é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso, sendo ativado antes que o sistema operacional esteja totalmente inicializado.

Questão 37 (FCC/TRE-SP/ANALISTA JUDICIÁRIO/ÁREA ADMINISTRATIVA/2017) Considere o texto abaixo.

Com efeito, nesse tipo específico de delito, o agente obtém, para ele ou outrem, vantagem ilícita (numerário subtraído de conta bancária), em prejuízo de alguém (a vítima, cliente de banco) mediante o emprego do artifício da construção de uma página eletrônica falsa ou envio de mensagem eletrônica (e-mail) de conteúdo fraudulento. Não haveria, como se disse, qualquer dificuldade de enquadramento do praticante do "ato ilícito" no art. 171 do CPC, impondo-lhe as sanções previstas nesse dispositivo (reclusão, de um a cinco anos, e multa). Além do mais, quando o criminoso implementa o último estágio da execução ilícita, que é a subtração não autorizada dos fundos existentes na conta da vítima, a jurisprudência tem entendido que aí está caracterizado o crime de furto qualificado, previsto no art. 155, § 4º, II.

(Adaptado de: REINALDO FILHO, Democrito. Disponível em: http://www.teleco.com.br/pdfs/tutorialintbank.pdf)

Hipoteticamente, um Analista Judiciário do TRE-SP identificou, corretamente, o ato ilícito referido entre aspas no texto como um tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. Comumente realizado por meio da internet, esse golpe é caracterizado como

a) identity theft.

b) fielding.

c) phishing.

d) hacker.

e) worming.

Letra c.

A questão aborda o Phishing (também conhecido como Phishing scam, ou apenas scam), que é um tipo de fraude eletrônica projetada para roubar informações particulares que sejam valiosas para cometer um roubo ou fraude posteriormente.

O golpe de phishing é realizado por uma pessoa mal-intencionada através da criação de um website falso e/ou do envio de uma mensagem eletrônica de conteúdo fraudulento. Utilizando de pretextos falsos, tenta enganar o receptor da mensagem e induzi-lo a fornecer informações sensíveis (números de cartões de crédito, senhas, dados de contas bancárias etc.).

Identity theft é o mesmo que falsa identidade.

Questão 38 (FCC/ALESE/TÉCNICO LEGISLATIVO/ TÉCNICO-ADMINISTRATIVO/2018)

Considere o trecho a seguir, retirado do Relatório de Crimes Cibernéticos da empresa Norton:

Vírus de computador e ataques de malware são os tipos mais comuns de crime cibernético que as pessoas sofrem, com 51% dos adultos sentindo os efeitos desses crimes mundialmente. Na Nova Zelândia, Brasil e China é ainda pior, com mais de 6 em 10 computadores infectados (61%, 62% e 65%, respectivamente). Os adultos em todo o mundo também são alvos de golpes (scams) online, ataques de phishing, roubo de perfis de redes sociais e fraude de cartão de crédito. 7% dos adultos até mesmo se depararam com predadores sexuais online.

(Disponível em: http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Portuguese-Hu man%20Impact-A4_Aug18.pdf)

O phishing, mencionado no texto, é um tipo de golpe por meio do qual um golpista

a) faz varreduras na rede do usuário, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles.

b) tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

c) armazena tudo o que o usuário digita pelo teclado do computador e depois obtém estes dados remotamente.

d) altera campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

e) utiliza um computador ou dispositivo móvel para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

Letra b.

A questão aborda o Phishing (também conhecido como Phishing scam, ou apenas scam), que é um tipo de fraude eletrônica projetada para roubar informações particulares que sejam valiosas para cometer um roubo ou fraude posteriormente.

O golpe de phishing é realizado por uma pessoa mal-intencionada através da criação de um website falso e/ou do envio de uma mensagem eletrônica de conteúdo fraudulento. Utilizando de pretextos falsos, tenta enganar o receptor da mensagem e induzi-lo a fornecer informações sensíveis (números de cartões de crédito, senhas, dados de contas bancárias etc.).

A palavra **phishing** (de fishing) vem de uma analogia criada pelos fraudadores, em que "iscas" (e-mails) são usadas para "pescar" informações sensíveis (senhas e dados financeiros, por exemplo) de usuários da Internet.

Questão 39 (FCC/ISS-TERESINA/AUDITOR FISCAL DO MUNICÍPIO/TI/2016) Um funcionário de uma empresa percebeu que seu computador estava sendo controlado remotamente sem seu consentimento, quando foi notificado pelo administrador da rede que, a partir de seu computador, estavam sendo enviados spams, realizados ataques de negação de serviço e propagação de outros códigos maliciosos. Com base nestas características e ações, conclui-se que o computador deve estar infectado por um

a) vírus.

b) rootkit.
c) keylogger.
d) spyware.
e) bot.

Letra e.

O computador do funcionário estava infectado por uma ameaça conhecida como “bot”.

De modo similar ao worm, bot é um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de software instalado em um computador. Adicionalmente ao worm, dispõe de mecanismos de comunicação com o invasor, permitindo que seja controlado remotamente. Os bots esperam por comandos de um hacker, podendo manipular os equipamentos infectados (conhecidos como máquinas Zumbis), sem o conhecimento e consentimento do usuário.

Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas na máquina contaminada, como desferir ataques de negação de serviço que impedem o uso de serviços online, furtar dados do computador infectado, enviar spams e realizar a propagação de outros códigos maliciosos.

Questão 40 (FCC/TRE-PB/TÉCNICO JUDICIÁRIO/ÁREA ADMINISTRATIVA/2015) Atualmente, a forma mais utilizada para a disseminação de vírus é por meio de mensagens de e-mails com anexos recebidos pela internet. Para que o vírus seja ativado:

a) é necessária a transferência do anexo para a Área de trabalho do computador.
b) é necessário que o anexo contaminado seja aberto ou executado.
c) basta realizar a abertura da mensagem para a sua leitura.
d) é suficiente o download da mensagem do servidor de e-mail para o computador.
e) é necessário que, uma vez aberta a mensagem, haja uma conexão com a internet.

Letra b.

Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja aberto ou executado.

Vírus propagado por e-mail: recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador.

Questão 41 (FCC/TRE-RR/ANALISTA JUDICIÁRIO/MEDICINA/2015) O processo de proteção da informação das ameaças caracteriza-se como Segurança da Informação. O resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco aspectos principais:

I – Somente as pessoas autorizadas terão acesso às informações.

II – As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.

III – Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

IV – Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

V – Garante que as informações foram produzidas respeitando a legislação vigente.

Os aspectos elencados de I a V correspondem, correta e respectivamente, a:

a) integridade - disponibilidade - confidencialidade - autenticidade –legalidade.

b) disponibilidade - confidencialidade - integridade - legalidade -autenticidade.

c) confidencialidade - integridade - disponibilidade - autenticidade -legalidade.

d) autenticidade - integridade - disponibilidade - legalidade –confidencialidade.

e) autenticidade - confidencialidade - integridade - disponibilidade -legalidade.

Letra c.

Aspectos de segurança	Descrição
confidencialidade	I – Somente as pessoas autorizadas terão acesso às informações.
integridade	II – As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.
disponibilidade	III – Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

autenticidade	IV – Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.
legalidade	V – Garante que as informações foram produzidas respeitando a legislação vigente.

Questão 42 (FCC/CNMP/ANALISTA DO CNMP/SUPORTE E INFRAESTRUTURA/2015) Alguns programas antivírus colocam arquivos suspeitos de possuírem vírus em quarentena, pelo fato de que não terem como combatê-los nesse momento. Um cuidado que o usuário do computador deve ter a partir de então, seguindo as recomendações dos programas antivírus, é de

a) reinstalar o sistema operacional, pois o possível vírus pode tê-lo contaminado, e não existem formas de reverter essa situação.

b) adquirir e instalar uma extensão do programa antivírus específica para o problema identificado.

c) apagar do computador todos os arquivos com a mesma extensão do arquivo colocado em quarentena, pois podem ter sido contaminados.

d) manter o programa antivírus sempre atualizado, na expectativa de que esse possível vírus possa ser identificado, e formas de combatê-lo desenvolvidas e incorporadas ao programa antivírus.

e) reinicializar o computador para que todos os efeitos desse possível vírus sejam anulados.

Letra d.

Ao encontrar um arquivo que o antivírus considera maligno, duas ações podem ser tomadas. A primeira envolve a eliminação da ameaça e a segunda consiste em colocar o arquivo em **quarentena,** em uma área em que o malware fica "afastado de suas funções" durante um tempo. O antivírus faz isso porque, caso a praga seja muito forte, sua remoção (por meio do processo de deletar) pode afetar todo o funcionamento do computador. Então, enquanto a mantém em quarentena, continua rodando o sistema em busca de mais problemas – todos eles ligados ou causados pelo vírus em quarentena.

Um cuidado que o usuário do computador deve ter a partir de então, seguindo as recomendações dos programas antivírus, é de manter o programa antivírus sempre atualizado, na expectativa de que esse possível vírus possa ser identificado, e formas de combatê-lo desenvolvidas e incorporadas ao programa antivírus, para que seja eliminado sem problemas.

Questão 43 (FCC/TCE-CE/ANALISTA DE CONTROLE EXTERNO/AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO/2015) Após o exame no computador do funcionário de uma instituição foi detectada sua participação em um ataque de DDoS sem seu conhecimento, em que seu computador atuava como um "zumbi", controlado remotamente por um atacante. Isso ocorreu porque o computador estava infectado por

a) adware.

b) rootkit.

c) bot.

d) spyware.

e) trojan.

Letra c.

O computador estava infectado por uma ameaça conhecida como "bot". De modo similar ao worm, é um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de software instalado em um computador.

Adicionalmente ao worm, dispõe de mecanismos de comunicação com o invasor, permitindo que o bot seja controlado remotamente. Os bots esperam por comandos de um hacker, podendo manipular os sistemas infectados, sem o conhecimento do usuário.

Segundo CertBr (2012), a comunicação entre o invasor e o computador pelo bot pode ocorrer via canais de IRC, servidores Web e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam.

Nesse ponto, cabe destacar um termo que já foi cobrado várias vezes em prova pela banca! Trata-se do significado de botnet, junção da contração das palavras robot (bot) e network (net). Uma rede infectada por bots é denominada de botnet (também conhecida como rede zumbi), sendo composta geralmente por milhares desses elementos maliciosos, que ficam residentes nas máquinas, aguardando o comando de um invasor.

Quanto mais zumbis (Zombie Computers) participarem da botnet, mais potente ela será.

Questão 44 (FCC/TRT-15ª/CAMPINAS-SP/ANALISTA JUDICIÁRIO/TI/2015) Sobre um programa de código malicioso – malware, considere:

I – É notadamente responsável por consumir muitos recursos devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho de redes e a utilização de computadores.

II – Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

III – Diferente do vírus, não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Os itens I, II e III tratam de características de um

a) Trojan Proxy.

b) Keylogger.

c) Scan.

d) Worm.

e) Spoofing.

Letra d.

a) Errada. Trojan Horse (Cavalo de Troia) é um programa aparentemente inofensivo que entra em seu computador na forma de cartão virtual, álbum de fotos, protetor de tela, jogo etc., e que, quando executado (com a sua autorização), parece lhe divertir, mas, por trás abre portas de comunicação do seu computador para que ele possa ser invadido.

b) Errada. Keylogger é um tipo específico de malware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Dentre as informações capturadas podem estar o texto de um e-mail, dados digitados na declaração de Imposto de Renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito. Em muitos casos, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site específico de comércio eletrônico ou Internet Banking. Normalmente, o keylogger contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de e-mails).

c) Errada. Varredura em redes, ou scan é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

d) Certa. Worm é a resposta dessa questão! Worms (vermes) são programas parecidos com vírus, mas que na verdade são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador (observe que os worms APENAS se copiam, não infectam outros arquivos, eles mesmos são os arquivos!). Além disso, geralmente utilizam as redes de comunicação para infectar outros computadores (via e-mails, Web, FTP, redes das empresas etc.). Diferentemente do vírus, o worm NÃO embute cópias de si mesmo em outros programas ou arquivos e NÃO necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

Worms são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias.

Difíceis de serem detectados, muitas vezes os worms realizam uma série de atividades, incluindo sua propagação, sem que o usuário tenha conhecimento. Embora alguns programas antivírus permitam detectar a presença de Worms e até mesmo evitar que eles se propaguem, isto nem sempre é possível.

e) Errada. Spoofing é uma prática em que um computador envia comandos a outro se fazendo passar por um terceiro.

Questão 45 (FCC/ALEPE/AGENTE LEGISLATIVO/2014) Um usuário fez o download de um programa gratuito para obter vídeos da Internet. Imediatamente após instalar o programa, o usuário notou que o seu navegador web passou a remetê-lo para a página inicial de um site indesejado, cheio de propagandas e informações sobre prêmios, sendo que essa página solicita de imediato alguns dados pessoais do internauta. Ele reeditou a informação da página

inicial do seu navegador, eliminando a página indesejada e substituindo-a pela de sua preferência. Surpreendentemente, a cada vez que o navegador era reiniciado ou quando era selecionada a abertura de uma nova página da Internet, o site indesejado voltava a ser exibido. Esse tipo de ocorrência refere-se a um

a) spyware, que está espionando a navegação do usuário com o objetivo de gerar informações relevantes para um hacker através da página redirecionada, que permitirá ao hacker o bloqueio remoto das ações do usuário.

b) trojan ou cavalo de troia que pode ter sido obtido no momento do download da aplicação para obter vídeos e em seguida ter sido executado pelo internauta.

c) sniffer, que tem por objetivo remeter o internauta para uma página web na qual onde os dados que ele digitar serão capturados por um cracker.

d) phishing, que falsifica a página principal do navegador, remetendo o internauta para outro endereço na internet.

e) worm hospedado no software que foi objeto de download, o qual tem por objetivo enviar os arquivos do usuário para um local na Internet acessado por um hacker.

Letra b.

O programa geralmente utilizado para exibição de propagandas é o Adware, que não se encontra listado nas opções. Outro ponto, é que o usuário baixou um programa que aparentemente seria para exibir vídeos da Internet, mas que na realidade faz a ação mencionada na questão. Então, esse fato nos remete ao cavalo de troia, letra “b”.

Questão 46 (FCC/ICMS-RJ/AUDITOR-FISCAL DA RECEITA ESTADUAL/2014) A política de segurança da informação da Receita Estadual inclui um conjunto de diretrizes que determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações. Dentre estas diretrizes encontram-se normas que garantem

I – a fidedignidade de informações, sinalizando a conformidade dos dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinalizam, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário, garantindo a não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.

II – que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, assegurando a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.

III – que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio das redes de comunicação, assegurando que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento.

Em relação às informações, as normas definidas em I, II e III visam garantir

a) fidedignidade, acessibilidade e disponibilidade.

b) integridade, disponibilidade e confidencialidade.

c) confidencialidade, integridade e autenticidade.

d) integridade, ininterruptibilidade e autenticidade.

e) confidencialidade, integridade e disponibilidade.

Letra b.

Item	Princípio	Característica
I	Integridade	É a garantia de que a informação que foi armazenada é a que será recuperada. A integridade busca proteção contra codificação não autorizada. Modificação deve ser realizada somente pelas partes devidamente autorizadas.
II	Disponibilidade	Busca acesso disponível às entidades autorizadas sempre que necessário.
III	Confidencialidade (ou sigilo)	É a garantia de que a informação não será conhecida por quem não deve. O acesso às informações deve ser limitado, ou seja, somente as pessoas explicitamente autorizadas podem acessá-las.

Questão 47 (FCC/AL-PE/ANALISTA LEGISLATIVO/INFRAESTRUTURA/2014) Os programas antivírus:

I – Protegem contra phishing de páginas web quando o usuário está em navegação utilizando livremente o browser.

II – Protegem contra trojan embarcado em uma aplicação quando o usuário aceita a sua instalação em sua máquina.

III – Criptografam comunicações em rede, sejam elas por meio de envio de mensagens ou navegação na Internet através de browser.

IV – Protegem contra códigos maliciosos embutidos em macros, as quais são utilizadas por um software aplicativo ou utilitário do computador do usuário.

V – Previnem a instalação de aplicativos infectados, no momento da solicitação de sua instalação, ao gerarem um alerta sobre conteúdo suspeito ou ao bloquearem a operação de instalação.

Está correto o que se afirma APENAS em:

a) I e II.

b) II e III.

c) III e IV.

d) IV e V.

e) II e V.

Letra d.

I – Errado. O tipo de golpe Phishing faz uso de pretextos falsos, na tentativa de enganar o receptor da mensagem, induzindo-o a fornecer informações sensíveis (como números de cartões de crédito, senhas, dados de contas bancárias etc.). O antivírus não atuará nesse caso.

II – Errado. O antivírus não irá proteger contra trojan (cavalo de troia) embarcado em uma aplicação quando o usuário aceita a sua instalação em sua máquina.

Trojan horse (Cavalo de troia): é um programa aparentemente inofensivo que entra em seu computador na forma de cartão virtual, álbum de fotos, protetor de tela, jogo etc., e que, quando executado (com a sua autorização!), parece lhe divertir, mas, por trás abre portas de comunicação do seu computador para que ele possa ser invadido.

III – Errado. As informações não são criptografadas com o antivírus.

IV – Certo. Faz proteção contra códigos maliciosos (malwares) embutidos em macros, as quais são utilizadas por um software aplicativo ou utilitário do computador do usuário.

V – Certo. Os antivírus previnem a instalação de aplicativos infectados, no momento da solicitação de sua instalação, ao gerarem um alerta sobre conteúdo suspeito ou ao bloquearem a operação de instalação.

Nota: Mesmo tendo um antivírus atualizado, isso não garantirá que o arquivo será identificado e bloqueado. Mas um antivírus atualizado aumenta as chances de detecção desses programas.

Questão 48 (FCC/ICMS-RJ/AUDITOR-FISCAL DA RECEITA ESTADUAL/2014) O site Convergência Digital divulgou a seguinte notícia: O Brasil segue como o no 1 na América Latina em atividades maliciosas e figura na 4ª posição mundial, ficando atrás apenas dos EUA, China e Índia, de acordo a Symantec. Os ataques por malwares cresceram 81%.... Um desses malwares segue sendo o grande vilão nas corporações, sendo responsável por mais de 220 milhões de máquinas contaminadas no mundo. É um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

(Adaptado de: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.ht m?infoid=34673&sid=18#.UlqcC-NKsiSo)

Considerando que o malware citado como vilão não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores, trata-se de um

a) vírus de macro.

b) botnet.

c) worm.

d) spyware.

e) backdoor.

Letra c.

a) Errada. Vírus de macro infecta documentos que contém macros. Mas o que é uma macro? Trata-se de um conjunto de comandos que são armazenados em alguns aplicativos e utilizados para automatizar tarefas repetitivas. Um vírus de macro é escrito de forma a explorar esta facilidade de automatização e é parte de um arquivo que normalmente é manipulado por algum aplicativo, como o Word, Excel, Powerpoint e Access, que utiliza macros. Para que o vírus de macro possa ser executado, o arquivo que o contém precisa ser aberto e, a partir daí, o vírus pode executar uma série de comandos automaticamente e infectar outros arquivos no computador.

b) Errada. Bot (Robô), de modo similar ao worm, é um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de software instalado em um computador. O termo botnet (junção da contração das palavras robot (bot) e network (net)) designa uma rede infectada por bots (também conhecida como rede zumbi), sendo composta geralmente por milhares desses elementos maliciosos que ficam residentes nas máquinas, aguardando o comando de um invasor.

c) Certa. Os **Worms** são programas parecidos com vírus, mas que na verdade são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador (observe que os worms apenas se copiam, não infectam outros arquivos, eles mesmos são os arquivos). Além disso, geralmente utilizam as redes de comunicação para infectar outros computadores (via e-mails, Web, FTP, redes das empresas etc.). Diferentemente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá pela execução direta de suas cópias ou através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

d) Errada. Spyware é um programa espião (spy em inglês = espião), que tem por finalidade monitorar as atividades de um sistema e enviar as informações coletadas para terceiros, sem o consentimento da parte envolvida.

e) Errada. Backdoor é uma brecha inserida em um sistema de computação que permite o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim, sem que seja necessário passar pelos sistemas de controle e autenticação implementados pelo administrador do sistema.

Questão 49 (FCC/TRT-18ª REGIÃO/GO/TÉCNICO JUDICIÁRIO/ TECNOLOGIA DA INFORMAÇÃO/2013) Em relação aos tipos de malware mencionados abaixo, é correto afirmar:

a) Rootkit é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

b) Backdoor é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.

c) Spyware é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes que exploram vulnerabilidades existentes nos programas instalados para invadi-lo.

d) Bot é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. Apesar de ainda serem bastante usados por atacantes, os bots atualmente têm sido também utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção.

e) Trojan ou trojan-horse, é um 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. Estes programas geralmente consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Letra e.

a) Errada. De modo similar ao worm, o bot é o programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de software instalado em um computador. Adicionalmente ao worm, dispõe de mecanismos de comunicação com o invasor, permitindo que seja controlado remotamente. Os bots esperam por comandos de um hacker, podendo manipular os sistemas infectados, sem o conhecimento do usuário.

b) Errada. Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes que exploram vulnerabilidades existentes nos programas instalados para invadi- lo.

c) Errada. Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.

d) Errada. Rootkit é uma forma de malware cuja principal intenção é se camuflar, para assegurar a sua presença no computador comprometido, impedindo que seu código seja encontrado por qualquer antivírus. Isto é possível porque esta aplicação tem a capacidade de interceptar as solicitações feitas ao sistema operacional, podendo alterar o seu resultado. O invasor, após instalar o rootkit, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador. Assim, permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

e) Certa. Trojan ou trojan horse são programas que entram no sistema escondidos atrás de ouros programas. O usuário recebe o programa imaginando que este é designado para uma determinada função, mas na realidade ele carrega outras instruções maliciosas. Muitas vezes o cavalo de troia abre uma brecha no sistema para que o autor invada a máquina ou envie informações privadas do usuário.

Questão 50 (FCC/TRE-CE/TÉCNICO JUDICIÁRIO/PROGRAMAÇÃO DE SISTEMAS/2012) Sobre segurança da informação, analise:

I – É obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

II – A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída aumenta a eficácia da implementação de um controle de acesso centralizado.

III – Os controles de segurança precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

IV – É importante para os negócios, tanto do setor público como do setor privado, e para proteger as infraestruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (e-gov) ou o comércio eletrônico (e-business), e evitar ou reduzir os riscos relevantes.

Está correto o que consta em

a) I, II, III e IV.

b) I, III e IV, apenas

c) I e IV, apenas.

d) III e IV, apenas.

e) I e II, apenas.

Letra b.

A única assertiva indevida é a II. A tendência da computação distribuída REDUZ a eficácia da implementação de um controle de acesso centralizado.

Questão 51 (FCC/TRT-11ª REGIÃO/PROVAS DE ANALISTA JUDICIÁRIO E TÉCNICO JUDICIÁRIO/2012) Quando o cliente de um banco acessa sua conta corrente através da internet, é comum que tenha que digitar a senha em um teclado virtual, cujas teclas mudam de lugar a cada caractere fornecido. Esse procedimento de segurança visa evitar ataques de

a) spywares e adwares.

b) keyloggers e adwares.

c) screenloggers e adwares.

d) phishing e pharming.

e) keyloggers e screenloggers.

Letra e.

O teclado virtual é uma forma de prevenção contra os programas maliciosos (malwares) keyloggers (capazes de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador) e screenloggers (que tentam coletar dados vindos da tela do computador). Portanto, a letra E é a resposta da questão!

Questão 52 (FGV/ALERJ/2017) Ataques cibernéticos podem causar graves prejuízos a pessoas e empresas. Recentemente João recebeu uma mensagem de alerta por e-mail com um pedido para ele atualizar seus dados cadastrais na página do seu Internet Banking.

João não prestou muita atenção em quem enviou a mensagem, nem se era um remetente confiável, e clicou no link presente no corpo do e-mail, que o levou para uma página web, replica do website real criada por um cyber criminoso.

Como a mensagem de e-mail e o website eram muito bem elaborados, João acreditou estar acessando algo verdadeiro e informou suas credenciais para acesso, quando na verdade ele as entregou a um criminoso.

João foi vítima de um ataque cibernético denominado:

a) DDoS;

b) sniffer;

c) spam;

d) phishing;

e) spoofing.

Letra d.

A questão destaca o Phishing (também conhecido como Phishing scam, ou apenas scam). É um tipo de fraude eletrônica projetada para roubar informações particulares que sejam valiosas para cometer um roubo ou fraude posteriormente. O golpe de phishing é realizado por uma pessoa mal-intencionada através da criação de um website falso e/ou do envio de uma mensagem eletrônica falsa, geralmente um e-mail ou recado através de scrapbooks como acontecia no Orkut, entre outros exemplos.

Utilizando de pretextos falsos, tenta enganar o receptor da mensagem e induzi-lo a fornecer informações sensíveis (números de cartões de crédito, senhas, dados de contas bancárias etc.).

Atualmente, este termo vem sendo utilizado também para se referir aos seguintes casos:

- mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;
- mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

Questão 53 (IADES/SEASTER-PA/TÉCNICO DE ENFERMAGEM/2019) Acerca dos procedimentos de segurança que devem ser adotados ao utilizar-se um computador, assinale a alternativa correta.

a) Não é recomendável utilizar CD-ROM para gravar cópias de arquivos.

b) Cópias de segurança de arquivos confiáveis devem ser feitas, mas somente em servidores on-line.

c) Qualquer arquivo importante deve ser copiado, seja ele confiável ou infectado.

d) Toda cópia de arquivo é confiável.

e) A manutenção de cópias de segurança redundantes de arquivos importantes é recomendável.

Letra e.

Backup ou cópia de segurança: é uma cópia de informações importantes que está guardada em um local seguro. Objetivo: recuperação de dados em caso de falha (perda dos dados originais); acesso a versões anteriores das informações.

Um **backup** envolve cópia de dados em um meio fisicamente separado do original, regularmente, de forma a protegê-los de qualquer eventualidade.

Para a realização de um backup, podemos utilizar: pen drive, CD, DVD, Blu-ray, HD externo, pastas compartilhadas na rede, armazenamento na nuvem ou "cloud storage" (uso do OneDrive - antigo SkyDrive, Dropbox, ou outro ambiente), Fitas-Dat etc.

Seja ele qual for a sua escolha, todos têm a mesma finalidade. A diferença está na capacidade, vida útil e segurança de cada um. Não é aconselhável o uso de outra partição do HD principal ou HD Interno, pois se acontecer algum problema com a máquina, todos os dados (originais e backup) serão perdidos.

Assim, copiar nossas fotos digitais, armazenadas no HD (disco rígido), para um DVD é fazer backup. Se houver algum problema com o HD ou se acidentalmente apagarmos as fotos, podemos então restaurar os arquivos a partir do DVD. Nesse exemplo, chamamos as cópias das fotos no DVD de cópias de segurança ou backup.

A cópia de segurança dos dados do usuário (ou *backup*), poderá estar corrompida quando for necessária a restauração.

Assim, uma das recomendações é manter cópias redundantes (duplicadas) de arquivos importantes. Por exemplo uma cópia pode estar em um HD local e a outra na nuvem. As chances de perda da cópia de segurança serão mínimas nesse contexto.

Questão 54 (IADES/SEASTER-PA/ENFERMEIRO/2019) Um spyware é um programa desenvolvido para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Com relação a esse assunto, assinale a alternativa correspondente a um programa que pode ser classificado como um spyware.

a) Rootkit

b) Backdoor

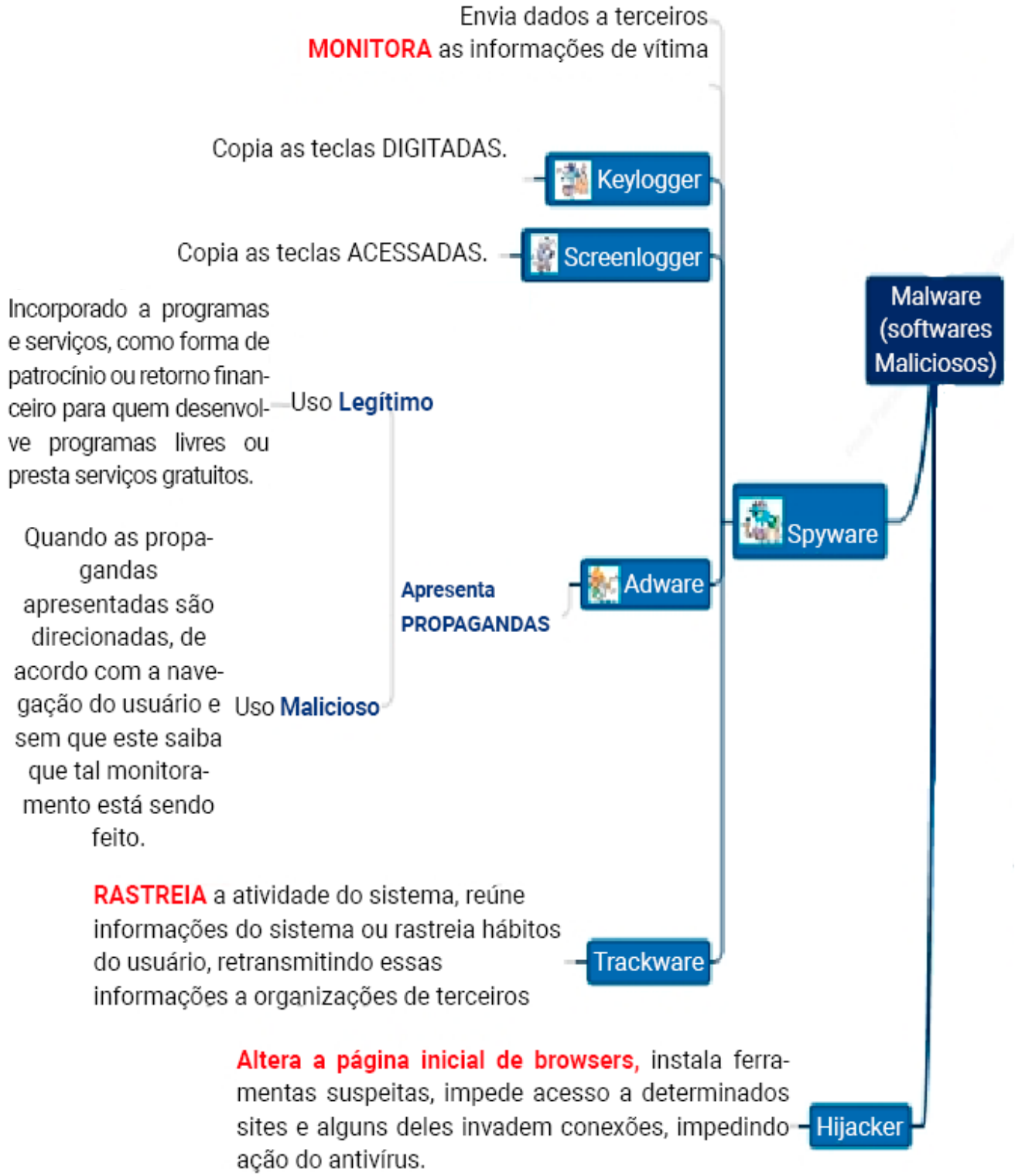
c) Adware

d) Vírus

e) Worms

Letra c.

Dentre as assertivas, a resposta correta é a letra “c”, conforme destacado a seguir no Mapa Mental.



Questão 55 (IADES/CAU-AC/AUXILIAR ADMINISTRATIVO/2019) A internet apresenta diversas ameaças ao usuário, que necessita ter atenção para navegar e não ser afetado. Entre elas, há a ameaça Spam, que pode ser definida como

a) o monitoramento das atividades do e-mail alvo.

b) um programa de computador que se propaga inserindo cópias de si mesmo.

c) a lixeira temporária do servidor de e-mails.

d) um programa instalado que se comunica com o invasor, para que este o controle à distância.

e) o envio não solicitado ou indesejado de e-mails a um grande número de pessoas.

Letra e.

Spam é um termo que designa qualquer mensagem de *e-mail*, independentemente de seu conteúdo, enviada para várias pessoas que não pediram para receber aquela mensagem. Ou seja, são mensagens não solicitadas, geralmente publicitárias, enviadas de forma massiva. O meio mais utilizado para o envio de spams é o correio eletrônico, mas também podem ser enviados por programas de mensagens instantâneas ou celulares.

Questão 56 (IADES/APEX BRASIL/ASSISTENTE/2018) O termo malwares, utilizado para se referir a programas maliciosos, nasceu da combinação das palavras, de língua inglesa, malicious e software.

Há um tipo de malware, normalmente recebido como um “presente” (por exemplo, um cartão virtual), que possibilita uma maneira de acesso remoto ao computador após a infecção e, além de executar as funções para as quais foi projetado, executa também outras funções normalmente danosas e sem o conhecimento dos usuários. O malware descrito é denominado de

a) screenlogger.

b) cavalo de Troia.

c) worm.

d) vírus.

e) backdoor.

Letra b.

a) Errada. Screenloggers são capazes de: armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.

b) Certa. Cavalo de Troia (ou Trojan Horse) é um programa, normalmente recebido como um "presente" (por exemplo cartão virtual, álbum de fotos, protetor de tela, jogo etc.), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

c) Errada. Worms são programas parecidos com vírus, mas que na verdade são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador (observe que os worms apenas se copiam, não infectam outros arquivos, eles mesmos são os arquivos!).

Veja as principais diferenças entre essas ameaças na tabela seguinte:

VÍRUS	WORM
É um programa (ou parte de um programa) que se anexa a um arquivo de programa qualquer.	Programa.
Propaga-se inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.	Não embute cópias de si mesmo em outros programas ou arquivos. Propaga-se automaticamente pelas redes, enviando copias de si mesmo de computador para computador.
Depende da execução do programa ou arquivo hospedeiro para ser ativado.	Não necessita ser explicitamente executado para se propagar. Basta que se tenha execução direta de suas cópias ou a exploração automática de vulnerabilidades existentes em programas instalados em computadores.

d) Errada. O vírus é um 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/ou arquivos.

e) Errada. O backdoor (porta dos fundos) é uma falha de segurança de um dado programa ou sistema operacional que permite a invasão de um dado sistema por um hacker de modo que ele obtém total controle do computador. Trata-se de um programa que, colocado no micro da vítima, cria uma ou mais falhas de segurança, para permitir que o invasor que o colocou possa facilmente "voltar" àquele computador em um momento seguinte.

REFERÊNCIAS

CERTBR. **Cartilha de Segurança para Internet**. Versão 4.0. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. 2012.

ALBUQUERQUE, R.; RIBEIRO, B. **Segurança no Desenvolvimento de Software**. Rio de Janeiro: Campus, 2002.

GEUS, Paulo Lício; NAKAMURA, Emilio Tissato. **Segurança de Redes em Ambiente Corporativos**. São Paulo: Novatec, 2007.

MAUSER, D; Diógenes, y. **Certificação Security +** - 2ª edição. 2013.

QUINTÃO, PATRÍCIA LIMA**. Tecnologia da Informação para Concursos.** 2020.

QUINTÃO, PATRÍCIA LIMA**. Informática para Concursos.** 2020.

QUINTÃO, PATRÍCIA LIMA. **Informática-FCC-Questões Comentadas e Organizadas por Assunto**, 3ª. Edição. Ed. Gen/Método, 2014**.**

QUINTÃO, PATRÍCIA LIMA. **1001 Questões Comentadas de Informática Cespe**, 2ª. Edição. Ed. Gen/Método, 2017.

RAMOS, A.; BASTOS, A.; LAYRA, A. **Guia Oficial para Formação de Gestores em Segurança da Informação**. 1. ed. Rio Grande do Sul: ZOUK. 2006.

STALLINGS, W., **Criptografia e Segurança de Redes: Princípios e Práticas**., 4. ed. São Paulo: Pearson Prentice-Hall, 2008.

SCHNEIER, B., **Applied Cryptography: Protocols, Algorithms and Source Code in C**. 2. ed. John Wiley & Sons, 1996.

Patrícia Quintão

Mestre em Engenharia de Sistemas e computação pela COPPE/UFRJ, Especialista em Gerência de Informática e Bacharel em Informática pela UFV. Atualmente é professora no Gran Cursos Online; Analista Legislativo (Área de Governança de TI), na Assembleia Legislativa de MG; Escritora e Personal & Professional Coach.

Atua como professora de Cursinhos e Faculdades, na área de Tecnologia da Informação, desde 2008. É membro: da Sociedade Brasileira de Coaching, do PMI, da ISACA, da Comissão de Estudo de Técnicas de Segurança (CE-21:027.00) da ABNT, responsável pela elaboração das normas brasileiras sobre gestão da Segurança da Informação.

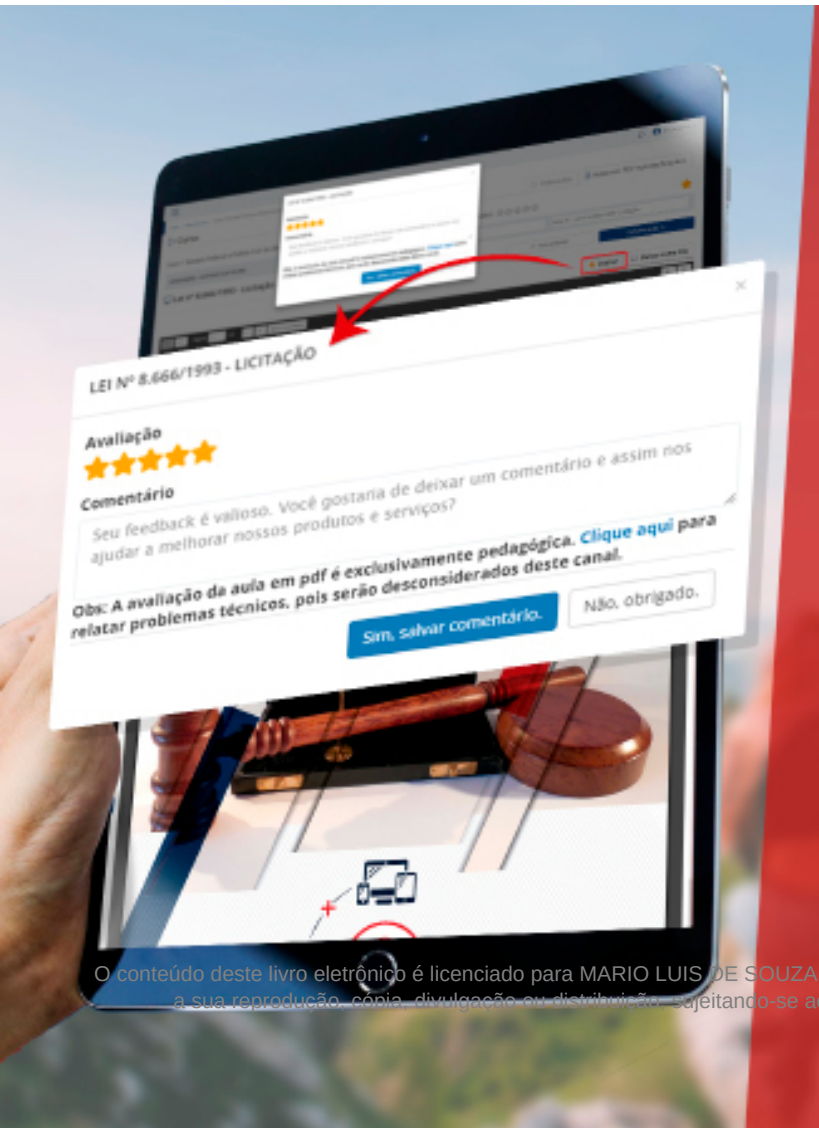
Autora dos livros: Informática FCC - Questões comentadas e organizadas por assunto, 3ª. edição e 1001 questões comentadas de informática (Cespe/UnB), 2ª. edição, pela Editora Gen/Método.

Foi aprovada nos seguintes concursos: Analista Legislativo, na especialidade de Administração de Rede, na Assembleia Legislativa do Estado de MG; Professora titular do Departamento de Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia; Professora substituta do DCC da UFJF; Analista de TI/Suporte, PRODABEL; Analista do Ministério Público MG; Analista de Sistemas, DATAPREV, Segurança da Informação; Analista de Sistemas, INFRAERO; Analista - TIC, PRODEMGE; Analista de Sistemas, Prefeitura de Juiz de Fora; Analista de Sistemas, SERPRO; Analista Judiciário (Informática), TRF 2ª Região RJ/ES, etc.

@coachpatriciaquintao
/profapatriciaquintao
@plquintao
t.me/coachpatriciaquintao

ANOTAÇÕES

ANOTAÇÕES



NÃO SE ESQUEÇA DE AVALIAR ESTA AULA!

SUA OPINIÃO É MUITO IMPORTANTE PARA MELHORARMOS AINDA MAIS NOSSOS MATERIAIS.

ESPERAMOS QUE TENHA GOSTADO DESTA AULA!

PARA AVALIAR, BASTA CLICAR EM LER A AULA E, DEPOIS, EM AVALIAR AULA.

AVALIAR