CURSO: Redes de Computadores

PROFESSOR (A): Marcus Vinicius

DISCIPLINA: INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO - ARA0064

ALUNO (A): LEONARDO AFONSO DA SILVA SOARES

TURMA: 3001 SALA: TEAMS DATA: 08 / 05 / 2021.

1ª Questão) Malware, ou "software malicioso," é um termo mais amplo que descreve qualquer programa ou código malicioso que seja prejudicial aos sistemas.

Hostil, intrusivo e intencionalmente prejudicial, o malware invade, danifica ou desabilita computadores, sistemas de computador, redes, tablets e dispositivos móveis, geralmente assumindo o controle parcial das operações de um dispositivo. Assim como a gripe para os humanos, ele interfere no funcionamento normal.

Tecnicamente, Cavalos de Tróia e Backdoors possuem semelhanças, mas por definição são diferentes. Apresente 01 semelhança e 01 diferença entre eles. (2,0 Pts)

Resposta:

Um backdoor é um software que permite o acesso remoto a um sistema (seja ele utilizado em dispositivos móveis ou não).Um exemplo do que seria um backdoor é como uma "entrada secreta" a um condomínio fechado, oculta para a maioria, no entanto, conhecida por poucos que podem aproveitar para entrar sem serem vistos e realizar suas ações.

Cavalo de Tróia é um tipo de malware que, frequentemente, está disfarçado de software legítimo. Eles podem ser empregados por criminosos virtuais e hackers para tentar obter acesso aos sistemas dos usuários.

As principais semelhanças entre eles é o fato de ambos poderem estar prejudicando o sistema sem mesmo o usuário saber, devido o fato de ambos poderem utilizar de métodos para não serem detectados.

Uma das diferenças é que os backdoors são instalados ou desenvolvidos nos sistemas, já o Cavalo de Tróia apenas carrega diversos vírus, podendo ter um backdoor.

2ª Questão) Toda informação possui um ciclo de vida. Um dado é gerado, permanece disponível pelo tempo necessário, passa por atualizações e, depois, ao perder sua serventia, deve ser descartado adequadamente. A sequência regular de início, meio e fim de uma informação pode ser uma forma de gerar conhecimento, mas se não for bem gerenciada, pode ser motivo de apreensão para os gestores.

Explique em poucas palavras como a correta utilização do ciclo de vida da informação pode gerar "CONHECIMENTO"(Pirâmide do Conhecimento). (2,0 Pts)

Resposta:

A informação e o conhecimento serão os diferenciais das empresas e dos profissionais que pretendem destacar-se no mercado e manter a sua competitividade.

Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais ou agregar custos, ou seja, não serão todas as informações e dados que necessitam ser arquivadas ou armazenadas por um determinado tempo.Por isso faz-se necessário saber qual a classificação da informação (podendo ser pública, interna, confidencial ou secreta) e descartar conforme a necessidade da organização, para assim disponibilizar espaço físico (menos papel, pasta, salas de arquivos e etc) quanto espaço virtual (armazenamento virtual, HDs, backups e etc) para novas informações, focando em dados e informações estratégica para as organizações.

3ª Questão) O man-in-the-middle (ou homem no meio) é uma forma de ataque em que os dados trocados entre duas partes, são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas se apercebam. Esse tipo de ataque pode ocorrer basicamente de 3 formas, sendo 2 ativas e 1 passiva.

Cite como são essas 3 formas, mostrando qual pilar da segurança da informação que cada um deles compromete. (2,0 Pts)

Resposta:

Ataques Man In The Middle de Wi-Fi geralmente assumem a forma de redes desonestas ou um "gêmeo mau".

> Redes desonestas são simplesmente rede Wi-Fi configuradas por cibercriminosos, completas com nomes sedutores como "Wi-Fi grátis" ou "Parece o Wi-Fi do Starbucks, mas não é".
>
> Ataques do gêmeo mau acontecem quando cibercriminosos configuram redes Wi-Fi públicas que imitam completamente redes legítimas que foram usadas no passado. Isso pode enganar seus dispositivos para se conectarem automaticamente, pois eles são projetados para facilitar sua vida e não precisar.

Assim, os cibercriminosos dominam essas conexões e quando as pessoas se conectam a elas, tudo que fazem passa pelos cibercriminosos. O cibercriminoso pode roubar suas senhas, dados de acesso e de pagamento, além de outros dados pessoais sigilosos.digitar senhas repetidamente.

No caso ambos estão ferindo a confidencialidade da informação, devido poderem apenas observar as informações na qual estão trocando.

Ataque Man In The Browser. MITB. MIB. Se resume a isso: um cavalo de Troia infecta seu dispositivo, permitindo que os criminosos entrem no meio de suas transações online (e-mails, pagamentos, serviços bancários, o que você tiver) e alterá-las para se adequar

às suas necessidades. Tudo isso sem você notar, pois o que você vê em sua tela é o que os cibercriminosos querem que você veja.

Já nesse ataque ele fere a confidencialidade e também a integridade, pelo fato de estar tendo acesso não autorizado a tal informação e pode também alterar a mesma.

4ª Questão) Não raro, ao se falar em segurança de informação no meio digital, isso é automaticamente associado a hackers, sistemas vulneráveis e vazamento de informação. Essa visão não está errada, contudo, esse é um assunto que pode ser um pouco mais complexo que bons antivírus e firewall.

Trata-se de sistemas, recursos, metodologias de armazenamento, compartilhamento e quaisquer ativos que sirvam para impedir que dados sejam acessados, alterados por pessoas não autorizadas ou ainda perdidos em desastres (que podem ser propositais).

Mas para alcançar esse objetivo, é preciso compreender e elevar a cultura interna para atender aos princípios básicos da segurança da informação.

Mostre os pontos de interligação dos Princípios da Segurança da Informação, com as Dimensões de Proteção da Informação, e o HEXAGRAMA PARKERIANO. (2,0 Pts)

Resposta:

Assim sendo, para referenciar o Hexagrama Parkeriano, poderíamos "brincar" com as letrinhas como numa sopa, assim: CIDAUP.

É preciso compreender ainda que, mesmo com mais atributos, as disciplinas de Segurança da Informação e Cibernética não se esgotam aqui. Temos por exemplo, a Legalidade como um atributo importante ao Tratamento/Processamento de Dados e isso jamais poderia ser ignorado em quaisquer das disciplinas, bem como o "Não-repúdio", que pode ser visto como uma técnica implementada para garantir que uma transação realizada não seja negada.

Compreendendo então que uma Violação de Dados (pessoais) é oriunda de um Incidente de Segurança (da Informação ou Cibernética), uma vez que este mesmo incidente envolve dados pessoais de pessoas singulares (e portanto, salvo exceções, protegidos por Lei), é possível discernir que, nem todo Incidente de Segurança é uma Violação de Dados, se não envolver dados pessoais.

5ª Questão) A necessidade de se manter as informações em segurança é tão antiga quanto a própria informação. No passado, imperadores colocavam guardas para proteger documentos oficiais e as igrejas mantinham seus documentos guardados a sete chaves. Com a explosão no uso dos computadores, os documentos ganharam o formato digital, e a internet passou a ser um grande veículo disseminador desse novo formato. Quanto maior o número de pessoas com acesso a determinada informação, maior sua vulnerabilidade. Com tanta informação circulando a velocidades de um

clique, não demorou muito para que houvesse a necessidade de se ter ferramentas capazes de autenticar, dar integridade, confidencialidade, disponibilidade e para certos tipos de documentos o não repúdio ou irretratabilidade da ação ou autoria de um ato nos documentos digitais. A utilização de assinaturas digitais em documentos eletrônicos com chaves criptográficas assimétricas e a utilização de certificados digitais gerados e gerenciados pôr em softwares livres ou gratuitos garantia a possibilidade da criação e verificação de documentos sem a necessidade de deslocamento a cartórios ou órgãos verificadores, sem perder a garantia da autenticidade. A assinatura digital tem sido um facilitador quando se trata de questões de segurança e digitalização de documentos. A figura abaixo demonstra um ciclo de criação de uma assinatura digital.

Explique como o receptor faz a verificação da assinatura digital do documento recebido.

Resposta:

A assinatura eletrônica do certificado é conferida pelo programa navegador (Internet Explorer,. Mozilla Firefox). O internauta precisa observar se o navegador realmente fechou o ícone do cadeado presente na barra inferior da sua janela, o que acontecerá ao entrar na área segura do site certificado. Ao clicar no cadeado, o próprio certificado é apresentado, e poderá então ser lido e conferido.

O software de assinatura também faz a verificação da validade do certificado digital utilizado, por meio de uma consulta (feita automaticamente) ao "site" da Autoridade Certificadora correspondente, onde são verificados a data de validade, os poderes de assinatura etc.

As três verificações (identidade do signatário, validade do certificado e integridade do conteúdo), acopladas à informação da data em que a assinatura foi feita, complementam o pacote de controles para garantir a segurança da transação.