Faculdade SENAC de Porto Alegre
Segurança em Sistemas – 2017/II
Prof. Filipo Mór
www.filipomor.com
Revisão para a Prova

Texto 1:

REDES SOCIAIS E SEGURANÇA DA INFORMAÇÃO

Em um mundo no qual a informação é um bem extremamente valioso, ganha pontos neste universo aquele que "tuíta" mais rápido, compartilha o quanto antes as fotos no Facebook, dissemina conteúdo de maior relevância nos blogs, divulga primeiro as melhores informações tidas como "furo de reportagem" e avisa instantaneamente os amigos onde está e o que está fazendo.

Esta convergência das mídias faz com que permaneçamos cada vez mais tempo conectados, interagindo com nossos amigos e contatos profissionais em tempo real através da Internet.

Como toda tecnologia, também há os prós e contras dessa "socialização digital". Dentre as vantagens, podemos citar: amigos a um clique de distância; migração dos meios analógicos para os digitais; interação do mundo "real" com o mundo "virtual"; maior compartilhamento de conhecimento; usuário passa a ser emissor de conteúdo, e não somente receptor; grande volume de informações divulgadas em maior velocidade; uso da rede como ferramenta para mobilização social; e rastreabilidade da informação (é possível conferirmos o autor de determinado conteúdo, em determinado dia e horário, e quais reflexos da publicação desse material).

Porém, há também os aspectos negativos desse comportamento: **(a)** excesso de exposição no mundo virtual; **(b)** cyberbullying; **(c)** limites entre privado e público passam a ser cada vez mais difusos; **(d)** confusão entre vida pessoal e profissional; **(e)** reputação negativa na Internet; **(f)** reflexos negativos no âmbito profissional; entre outros. [...]

Gisele Truzzi, http://www.truzzi.com.br/pdf/artigo-redes-sociais-e-seguranca-da-informacao.pdf, acessado em 19/jun/2017.

1. Explique os aspectos negativos citados pela autora (itens de *a* até *f*), dando exemplos e indicando formas de mitigação ou mesmo de evitá-los completamente.

Texto 2:

Cyberbullying: a violência virtual.

[...] você vai entender os três motivos que tornam o *cyberbullying* ainda mais cruel que o bullying tradicional.

- No espaço virtual, os xingamentos e as provocações estão **(a)** permanentemente atormentando as vítimas. Antes, o constrangimento ficava restrito aos momentos de convívio dentro da escola. Agora é o tempo todo.

- Os jovens utilizam cada vez mais ferramentas de internet e de **(b)** troca de mensagens via celular - e muitas vezes se expõem mais do que devem.

- A tecnologia permite que, em alguns casos, **(c)** seja muito difícil identificar o(s) agressor(es), o que aumenta a sensação de impotência.

Beatriz Santomauro, https://novaescola.org.br/conteudo/1530/cyberbullying-a-violencia-virtual, acessado em 19/jun/2017.

2. Como as vitimas acabam sofrendo um atormentamento permanente (a)? Explique quais os aspectos técnicos relacionados a forma como uma informação pode se tornar perene no ambiente virtual.
3. Recentemente ocorreram episódios de indisponibilização de alguns serviços de troca instantânea de mensagens, a partir de ordens judiciais. Comente, sob o aspecto técnico, a viabilidade de se "bloquear" este tipo de serviço. Explique, ainda, como funciona a segurança neste tipo de aplicativo, lembrando que normalmente estes dependem de comunicação através de um servidor, com criptografia ponta a ponta.
4. Comente, sob o aspecto técnico, a viabilidade (ou falta dela) no monitoramento do conteúdo de mensagens de aplicativos de troca instantânea.

5. Explique o funcionamento dos seguintes softwares maliciosos:
    a. Keylogger
    b. Ransonware
    c. Virus
    d. Worm
    e. Cavalo de Troia (trojan)

6. Relacione as colunas:

1 – Teoria do Perímetro.	**( )** Quanto menos informações um agente tiver a respeito do ambiente alvo, maior será a sua dificuldade em invadi-lo.
2 - Estratégia de proteção: ponto de estrangulamento.	**( )** Aplicação de defesas distintas, de controles complementares como redundância, para no caso de falha ou violação de um, haja outro controle e não torne o sistema como um todo vulnerável e restrito a somente um único controle.
3 - Estratégia de proteção: defesa em profundidade.	**( )** Têm por objetivo tornar o custo da invasão maior do que o valor da informação.
4 - Estratégia de proteção: segurança pela obscuridade.	**( )** Resistência distribuída por espaços físicos e lógicos.
5 - Barreiras de proteção.	**( )** Estratégicas em um mesmo ponto de controle em que passem todos os usuários.

7. Explique os seguintes tipos de ataques: **negação de serviço**, **homem do meio**, ***phishing***, ***spoofing*** e **sequestro de sessão**.
8. Como funciona a filtragem de pacotes?
9. O que é uma DMZ? Como funciona?
10. O quê são e como funcionam as Redes Privadas Virtuais?
11. Como funciona um ataque de DDoS?
12. Quais os objetivos da segurança da informação? Explique-os.
13. O quê é um firewall? Para quê serve? E quais os tipos existentes?
14. Conceitue os seguintes termos, dentro do contexto da área de Segurança da Informação: ativo de informação, escopo, ameaça, proteção, risco, vulnerabilidade, incidente.
15. Considere o algoritmo de criptografia assimétrica RSA. Quais das seguintes afirmações são verdadeiras?
    a. ( ) A etapa de codificação exige maior poder computacional do que a etapa de decodificação.
    b. ( ) Bibliotecas tradicionais (como por exemplo, *math.h*) são insuficientes para a execução do algoritmo.
    c. ( ) O algoritmo exige a utilização de números primos “grandes”, com pelo menos 100 digitos.
    d. ( ) Os números primos p e q, escolhidos para a geração das chaves, definem, entre outras coisas, o tamanho do bloco.
    e. ( ) É possível decifrar a chave privada a partir da chave pública.
    f. ( ) Chaves compostas por512 bits são consideradas seguras.