FACULDADE PITÁGORAS

PRONATEC

DISCIPLINA: SEGURANÇA DA INFORMAÇÃO

Prof. Msc. Carlos José Giudice dos Santos

Conteúdo Programático

Unidade 01
Por que Segurança da Informação

- Conceitos gerais
- Princípios fundamentais de segurança
- Informação
- Sistemas de informação
- O que são bancos de dados
- Log
- Sociedade e segurança da informação

Por que Segurança da Informação [01]

A Era da Informação

- A sociedade pós-industrial
- A sociedade pós-capitalista
- A sociedade informacional
- A sociedade digital

Por que Segurança da Informação [2]

A Era da Conectividade

- "Penso, logo existo"
- "Estou conectado, logo existo"
- Condições para não ser um excluído na sociedade digital

Por que Segurança da Informação [3]

A Informação

- Importância da informação
- Bancos de dados
- Ameaças, vulnerabilidades e fragilidades
- Sistemas de informação
- Comércio eletrônico
- Mercado de trabalho para o profissional de segurança da informação

Princípios Fundamentais de Segurança [1]

A Tríade CIA

- Confidencialidade (Confidentiality)
- Integridade (Integrity)
- Disponibilidade (Availability)

Princípios Fundamentais de Segurança [2]

Confidencialidade

- Confidencialidade é a capacidade de garantir o nível de sigilo necessário a cada junção (ou ponto) de dados em processamento.

- Confidencialidade é a capacidade de prevenir a divulgação não autorizada de dados ou informações.

Princípios Fundamentais de Segurança [3]

Ameaças à Confidencialidade

- Monitoramento de rede
- "Surf de ombro"
- Engenharia Social
- Roubo de arquivos de senhas

Princípios Fundamentais de Segurança [4]

Como garantir a Confidencialidade

- Criptografia de dados (na armazenagem e transmissão)
- Monitoramento do tráfego de rede
- Controle de acesso rigoroso
- Classificação dos dados (quanto ao nível de segurança)
- Treinamento dos usuários do sistema

Princípios Fundamentais de Segurança [5]

Integridade

- É a garantia de que não haverá modificações não autorizadas de dados e/ou informações.

- A integridade depende do rigor da confiabilidade.

Princípios Fundamentais de Segurança [6]

Como garantir a Integridade

- Mecanismos de hardware, software e comunicação trabalhando juntos para garantir manutenção, processamento e transmissão de dados e/ou informações sem qualquer alteração não autorizada ou não esperada.
- Proteção dos sistemas da empresa contra interferências e contaminações externas ao seu ambiente tecnológico.

Princípios Fundamentais de Segurança [7]

Disponibilidade

- É a capacidade que sistemas e redes devem ter para disponibilizar dados de forma previsível e adequada às necessidades de seus usuários.

- Qualquer falha na disponibilidade deve ser reparada de forma rápida e segura para não comprometer a produtividade dos sistemas e das redes.

Princípios Fundamentais de Segurança [8]

Como garantir a Disponibilidade

- Mecanismos de backup
- Proteção elétrica
- Proteção ambiental
- Proteção contra ataques lógicos (invasões, por exemplo – DoS)

Informação [1]

Diferença entre dados e informações

- Dados são fatos isolados, com pouco ou nenhum significado, porque não passaram ainda por um processo de interpretação
- Dado é uma representação ou um registro de uma informação
- Dados são geralmente quantificáveis e podem ser facilmente obtidos por meio de máquinas

Exemplos de dados:

1. Temperatura atual = 38° ;
2. Velocidade Média na avenida principal agora = 5 km/h;
3. Pressão atmosférica caiu muito nos últimos 30 minutos.

Informação [2]

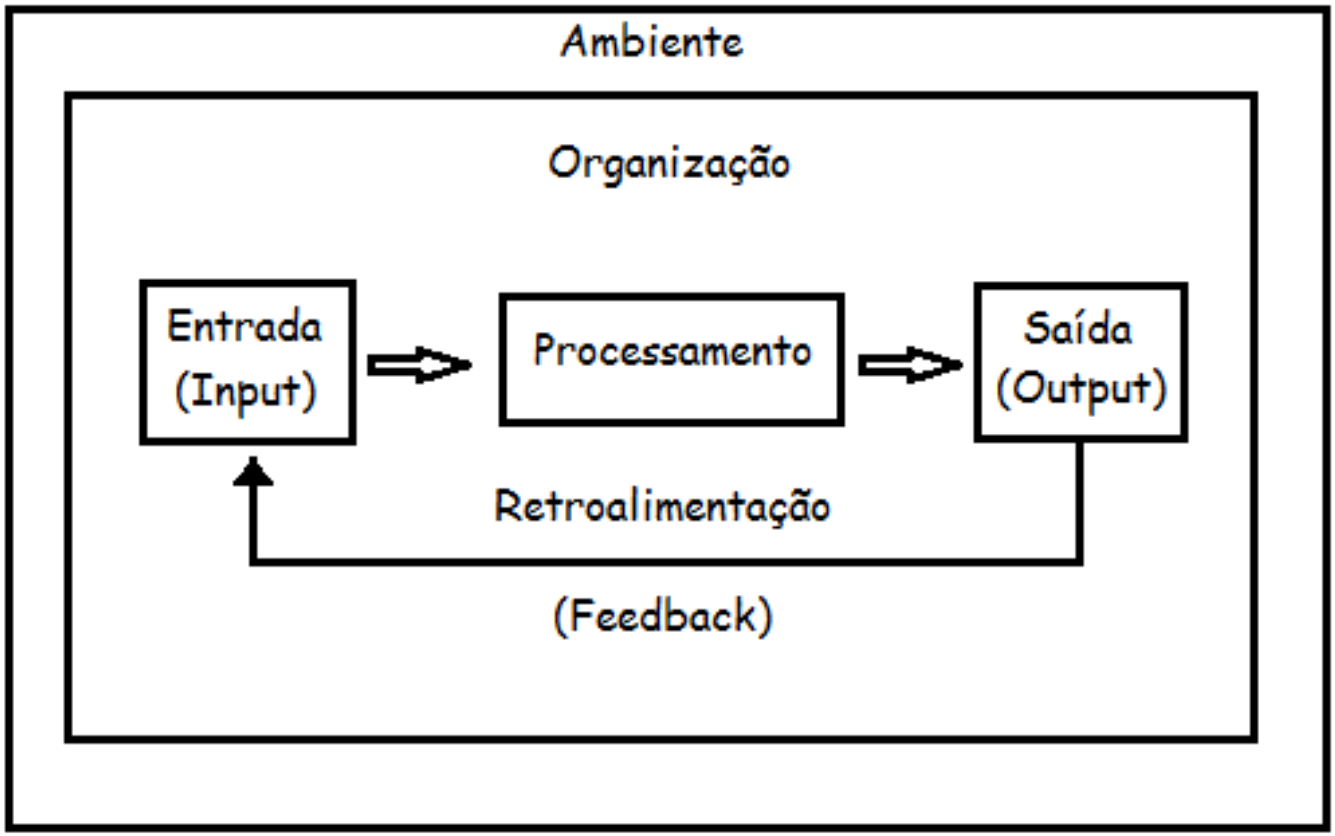
Diferença entre dados e informações

- Informação é um dado contextualizado e interpretado, que tem o objetivo de responder perguntas
- Para se obter informação é necessária a mediação humana direta (análise) ou indireta (processamento de dados)
- Informação é um dado dotado de significado e propósito.

Exemplos de informação

1. Hoje está quente
2. O trânsito na avenida principal está muito congestionado agora
3. Uma tempestade se aproxima agora

Sistemas de Informação [1]



Atividades de um sistema de informação

Sistemas de Informação [2]

- **Entrada**: parte do SI responsável em coletar dados de dentro da organização ou de seu ambiente externo. A entrada pode ser composta de dados, informações ou eventos – que podem ser chamados de requisitos.
- **Processamento**: parte do SI responsável em transformar os dados brutos em informações – é composto por normas e procedimentos
- **Saída**: parte do sistema responsável em transferir as informações processadas às pessoas ou atividades em que serão empregadas – leva à uma ação ou evento.
- **Feedback**: é a parte do sistema de informação que fornece uma resposta com o objetivo de avaliar, corrigir ou otimizar o estágio de entrada.
- **Ambiente**: local onde está inserida a organização, sendo composto por fornecedores, clientes, acionistas, concorrentes e agências reguladoras.

Sistemas de Informação [3]

Os sistemas de informação são complexos porque não compreendem apenas os programas como muita gente pensa.

Pode-se dizer que os SI's possuem dois componentes básicos:

- **Componente social**: formado pelas pessoas e pelos processos criados por essas pessoas (processos organizacionais) que exprimem a cultura da organização.
- **Componente tecnológico**: composto pelas tecnologias da informação e da comunicação, o que inclui hardware (computadores, impressoras, redes, etc) e software (sistemas operacionais, aplicativos, bancos de dados, etc).

Bancos de Dados [1]

Um banco de dados pode ser definido como um conjunto de dados devidamente relacionados. Um banco de dados possui as seguintes propriedades:

- É uma coleção lógica coerente de dados com um significado inerente; uma disposição desordenada dos dados não pode ser referenciada como banco de dados.
- Ele é projetado, construído e preenchido com valores de dados para um propósito específico; um banco de dados possui um conjunto predefinido de usuários e de aplicações.
- Ele representa algum aspecto do mundo real, chamado de minimundo; os SI's processam dados que geralmente estão armazenados em bancos de dados.

Bancos de Dados [2]

Antes somente era considerado banco de dados uma coleção lógica coerente de dados com um significado inerente e disposta de forma ordenada. Uma disposição desordenada de dados, por sua vez, não era considerada um banco de dados.

Hoje, entretanto, dados não estruturados e até mesmo desordenados são considerados banco de dados, pois caracterizam o que se denomina dados não estruturados.

São, ainda, considerados extremamente importantes, afinal, o contexto das redes sociais é formado por esse tipo de estrutura de dados.

Podem ser considerados bancos de dados: arquivos de texto, planilhas eletrônicas e estruturas de sistemas gerenciadores de bancos de dados (tabelas).

LOG [1]

Quando o capitão de um navio escreve o diário de bordo (em inglês, *log*), ele registra os principais fatos ocorridos na embarcação. Ele está na realidade fazendo este registro para a qualquer momento da navegação revisar o que aconteceu durante o período.

Da mesma maneira, os SI's e todos os sistemas relacionados (redes e bancos de dados) realizam constantemente o *log* de toda e qualquer operação ocorrida continuamente. Dessa maneira, eles garantem que todas as informações sejam registradas, informando quem acessou, quando, como, o valor da informação e que operação foi realizada.

O registro de log permite, em caso de perda de dados, que os SI's possam recuperar estes dados a partir do momento anterior à ocorrência da perda.

SOCIEDADE E SEGURANÇA DA INFORMAÇÃO [1]

Não seria exagerado afirmar que as informações na sociedade dependem cada vez mais dos sistemas de informação e da utilização de computadores pessoais e equipamentos móveis. E, por isso, interpretamos a segurança da informação como assunto diretamente relacionado com a tecnologia da informação.

Diariamente há notícias nos jornais, telejornais e portais de notícias dando conta de crimes cibernéticos praticados por indivíduos conhecidos como hackers.

Classificar um hacker como criminoso é um engano comum que deve ser combatido. Hacker é uma pessoa que estuda, em profundidade, como modificar os aspectos internos de dispositivos de tecnologia da informação, programas e redes de computadores.

SOCIEDADE E SEGURANÇA DA INFORMAÇÃO [2]

Às vezes, o conceito de hacker se confunde com um outro tipo de estudioso com as mesmas capacidades, mas com objetivos diferentes. Trata-se dos crakers.

Segundo a definição correta, hacker é aquele indivíduo que se preocupa em utilizar seu conhecimento para detectar e melhorar falhas e vulnerabilidades de sistemas de informação e redes de computadores.

Por outro lado, existem os crackers e outros tipos de usuários com grande conhecimento, que não tem preocupação em usar as técnicas que desenvolvem ou aprendem de maneira ética – buscam seus próprios interesses.

Vamos aprender mais sobre os tipos de hackers que existem. As definições a seguir são baseadas no Curso Básico de Hacker, disponível em www.passwordtechnology.com.br

TIPOS DE HACKERS: LAMMER [1]

Significa "otário" na língua inglesa. Algumas pessoas consideram que **lammer** é uma denominação para o hacker iniciante. Este é um conceito equivocado.

Lammers são indivíduos que "pensam" ser **hackers** e que costumam utilizar programas maliciosos (vírus, trojans, spywares, etc) desenvolvidos por **crackers** para sacanear usuários leigos.

Os **lammers** não são bem vistos pela comunidade hackers e não possuem acesso ao verdadeiro conhecimento. Os **lammers** simplesmente fazem download de programas maliciosos e assistem alguma videoaula que ensina a utilizar este tipo de programa, para então, prejudicar outras pessoas.

TIPOS DE HACKERS: NEWBIE [2]

Newbie é o novato no conhecimento **hacker**. Em fóruns de discussão, os **newbies** são conhecidos pela sigla **NB** que significa que são **hackers** principiantes.

Um **newbie** tem sede de conhecimento (quer sempre saber mais) e geralmente pergunta o tempo todo. Seu objetivo é acumular tanto conhecimento quanto for possível para um dia tornar-se **hacker**.

Em salas de bate-papo e salas de jogos on-line, o **newbie** é também conhecido como **NOOB**, ou seja, um novato que está no início de uma carreira para tornar-se **hacker**.

Algumas vezes este termo é utilizado como chacota pelos veteranos. Nunca se deve confundir um **newbie** com um **lammer**, pois o **newbie**, por mais inconveniente que seja, é apenas um aprendiz que não tem o objetivo de prejudicar ninguém.

TIPOS DE HACKERS: WANNABIE [3]

Wannabie é o sucessor do **newbie** no mundo **hacker**. Os **wannabies** geralmente utilizam programas desenvolvidos por usuários mais experientes (do tipo força bruta, exploits, portscanners, etc), desconhecendo alguns princípios da ética hacker.

Estes programas são utilizados para seu aprendizado e/ou reconhecimento social e para testar os seus conhecimentos.

Este é o segundo passo para tornar-se um hacker.

TIPOS DE HACKERS: WORM [4]

Também conhecidos como **larvas**, os **worms** são usuários com um nível maior de conhecimento que os **wannabies**.

Eles já conseguem modificar aplicativos prontos e/ou desenvolver seus próprios programas. Em alguns casos, podem até conseguir invadir servidores de pequeno ou médio porte, que possuem falhas de segurança.

O **worm** é o terceiro passo para tornar-se um hacker ou um cracker.

TIPOS DE HACKERS: SCRIPT KIDDIE [5]

Os **script kiddies** podem ser definidos como usuários que estão em busca de um alvo fácil. Seu objetivo é conseguir o acesso root (aquele que tem o privilégio de administrador de sistema) da maneira mais fácil possível.

Geralmente fazem isso concentrando-se em um pequeno número de exploits e então, procuram pela internet por alguma máquina que possua vulnerabilidades a serem exploradas.

Em termos de conhecimento, estão acima dos **lammers** e em geral, desconhecem a ética hacker.

TIPOS DE HACKERS: CRACKER [6]

Os **crackers** são os principais responsáveis pelo preconceito que existe sobre os **hackers**.

São usuários com grandes conhecimentos de informática (especialmente na área de redes e de programação de computadores), que fazem mal uso de seus conhecimentos.

São geralmente conhecidos como **hackers** maus, que cometem crimes digitais (como invasão de não autorizada de sistemas, de contas bancárias, roubo e uso de informações pessoais, deformação de sites e outros tipos de crimes).

Pode-se definir os **crackers** como **hackers** que escolheram fazer mal uso de seus conhecimentos. Os **crackers** quebram senhas de provedores, senhas de proteção de jogos, lançam versões falsas de programa e de sistemas e são responsáveis por todos tipos de crime digitais.

TIPOS DE HACKERS: DEFACER [7]

Os **defacers** são **crackers** especializados em invadir provedores de hospedagem de sites com o objetivo de desfigurar a página principal de um determinado site.

Seria algo como o correspondente cibernético dos pixadores de muros e fachadas do mundo real.

Defacements acontecem geralmente em sites famosos, sempre com o intuito de conseguir algum tipo de publicidade para seus objetivos.

TIPOS DE HACKERS: CARDER [8]

Os **carders** são **crackers** especializados em roubar senhas de cartão de crédito e de acesso a bancos, seja através de programas (do tipo trojan) ou por aparelhos conhecidos como chupa-cabra.

Quando os carders conseguem este tipo de informação, utilizam para o seu próprio bem ou vendem estas informações por dinheiro.

Estas transações (troca ou venda de senhas) ocorrem em bate-papos ocultos.

TIPOS DE HACKERS: PHREAKER [9]

Os **phreakers** são **crackers** especializados em telecomunicações. Basicamente, são aqueles que utilizam os seus conhecimentos para fraudes utilizando linhas telefônicas fixas, móveis ou modems.

Os **pheakers** (**crackers** da telefonia) burlam métodos de ligações, alteram sistemas telefônicos, roubam informações e são capazes de ligar de graça para qualquer lugar.

O QUE É UM HACKER [1]

Hackers são pessoas que se dedicam, com uma intensidade fora do normal, a conhecer determinadas áreas da informática, especialmente a área de redes, segurança digital e de linguagens de programação.

Para um **hacker**, não existem limites para a busca de conhecimento. Os conhecimentos adquiridos pelos **hackers** podem ser utilizados para diversos propósitos.

Uma definição comum de **hacker** é "pessoa com grande conhecimento de informática, e que utiliza deste conhecimento para benefício de pessoas que usam um sistema, ou contra elas".

O QUE É UM HACKER [2]

A origem etimológica da palavra **hacker** vem do verbo "**to hack**" da língua inglesa, que significa "cortar".

Este termo está relacionado ao fato de se desenvolver uma técnica dentro de um certo âmbito, para contornar ou achar um atalho não previsto nas configurações normais.

Hack em inglês tem o significado de "gambiarra", uma solução original ou paliativa para se resolver um problemas ou burlar alguma regra.

Foi usado inicialmente por ferromodelistas da década de 50, que promoviam modificações nos relés eletrônicos de controle dos trens e de ferrovias para modificar.

Posteriormente, na década de 60, passou a ser utilizado pelo pessoal da computação para designar truques engenhosos de programação.

O QUE É UM HACKER [3]

O termo hacker é motivo para muita polêmica e discussões, porque durante muito tempo e muitas vezes, até hoje, todo tipo de crime cibernético divulgado pela mídia é geralmente atribuído aos hackers ou cyber criminosos.

Ser hacker não é crime. Ser hacker é ter um conhecimento excepcional sobre informática, e na maioria dos países, ter ou obter conhecimento não é proibido. O que é proibido é fazer mau uso do conhecimento.

Saber como invadir um sistema, um programa ou um banco não é crime. O hacker ético quando faz isso, tem autorização para fazê-lo e as técnicas utilizadas são conhecidas como "penetration test", e tem o objetivo de identificar vulnerabilidades e prevenir ameaças de segurança aos sistemas.

Invadir sem autorização é um crime praticado por crackers.

NEWS: SEGURANÇA DA INFORMAÇÃO [1]

No início dos anos 2000, falou-se muito sobre sistemas e espionagem digital em massa promovido por países ligados aos EUA. Naquela época, o suposto sistema de espionagem mundial era conhecido como ECHELON (SCHNEIER, 2001).

Estes rumores não foram confirmados, até que em 2013, aconteceu o caso Snowden. Um ex-funcionário da NSA (National Security Agency) chamado Edward Snowden revelou que era responsável em operar um sistema chamado Prism para espionar e acompanhar todo tipo de informação (pessoais, comerciais e industriais) para a NSA, com a colaboração das maiores empresas digitais do mundo (telefônicas, Facebook, Microsoft, Apple, Google, entre outras).

O sistema Prism iniciou suas operações em 2007 e forneceu um acesso sem precedentes do governo americano a informações pessoais.

NEWS: SEGURANÇA DA INFORMAÇÃO [2]

Como funciona o sistema Prism?

- O Prism é na verdade uma sigla para um programa real do governo dos Estados Unidos. De acordo com documentos vazados, ele entrou em ação em 2007, e só ganhou força desde então.
- A sua finalidade é monitorar potenciais comunicações estrangeiras valiosas que podem passar pelos servidores dos Estados Unidos, mas parece que na prática seu alcance é bem maior.
- Os relatos iniciais sugeriam que o processo funcionava da seguinte maneira: as empresas digitais mencionadas (e talvez até outras) recebiam uma diretiva do procurador-geral e do diretor de inteligência nacional.

NEWS: SEGURANÇA DA INFORMAÇÃO [3]

- Elas davam acesso aos seus servidores através da Unidade de Tecnologia de Interceptação de Dados do FBI, a qual por sua vez os retransmitia para os escritórios de tecnologia da NSA.
- Ainda existem, como você deve imaginar, filtros para ajudar a lidar com a quantidade de dados recebidos diariamente, os trilhões de bits e bites que fazem sua identidade e vida online.
- Alguma coisa para garantir que apenas os caras maus estão sendo vigiados (será?), e não os cidadãos honestos. Existe sim um filtro, e é ridículo: um analista da NSA precisa ter 51% de certeza de que um assunto é "externo". Depois disso, carta branca.

NEWS: SEGURANÇA DA INFORMAÇÃO [4]

O que é mais preocupante sobre o PRISM não é a coleta de dados. É o tipo de dado coletado.

De acordo com o artigo do Washington Post, isso inclui:

> …conversas por vídeo e áudio, fotografias, e-mails, documentos e logs de conexão…[Skype®] podem ser monitorados por áudio quando um dos lados da conversa é em um telefone convencional, e para qualquer combinação de 'áudio, vídeo, chat, e transferência de arquivos' quando os usuários do Skype® se conectam por um computador.

O disponibilizado pelo Google inclui Gmail, chats de voz e vídeo, arquivos do Google Drive, bibliotecas de fotos e vigilância de termos de busca em tempo real. Imagine o quanto de suas informações estão acessíveis nesta situação.

NEWS: SEGURANÇA DA INFORMAÇÃO [5]

A mesma profundidade similar de acesso também se aplica ao Facebook, Microsoft e ao resto.

Para sermos mais claros: isso abrange praticamente qualquer coisa que você já tenha feito online, e ainda inclui pesquisas no Google® **enquanto** você está digitando.

Quando a NSA monitora registros de telefone, ela só coleta os metadados deles. Isso significa quem e para quem a chamada foi feita, e de onde ela foi feita, e outras informações gerais. É importante entender que, até onde sabemos, o conteúdo das conversas não era monitorado ou registrado.

Em contraste, o PRISM pelo noticiário geral que se tem acesso permite acesso total não apenas ao fato de que um e-mail foi enviado – ele permite acesso ao conteúdo destes e-mails e chats.