Segurança da Informação

Aula 03

Aula 03

Riscos envolvendo informações:

"O maior risco é crer que não há riscos"

Caruso & Steffen

Os riscos agravaram-se após:

- a centralização da informação ;
- o grande volume de informações ;
- o aparecimento dos microcomputadores, redes, internet, e disseminação da cultura de informação.

Aula 03

Segurança da Informação

Microcomputadores, apesar de possuírem praticamente os mesmos recursos presentes em computadores de grande porte, têm de ser tratados de forma um tanto diversas no que se diz respeito à segurança.

A razão para isso reside exatamente no seu reduzido tamanho, maior facilidade de uso e preço relativamente baixo, o que provocou sua disseminação e interconexão em massa.

Aula 03

Segurança da Informação

Concentração de informações

- Antes do advento dos computadores

  → Existia a necessidade de se dispor dos dados necessários de forma centralizada e rápida.

- Após o advento dos computadores

  →Tornaram o problema mais crítico ao multiplicar muitas vezes a quantidade de informações que pode ser armazenadas em espaços restritos.

  (facilitando a exclusão dos dados em pequenos equipamentos e internet)

Aula 03

Segurança da Informação

Acesso indiscriminado

Ainda que os CPD's estejam sendo "escondidos" e protegidos em números cada vez maior, persistem os casos de CPD's ou servidores de redes em ambientes de fácil acesso.

Como por exemplo a sinalização visual indicando claramente o acesso à sala do servidor.

Mais grave que o acesso físico é o acesso lógico às informações.

Aula 03

Segurança da Informação

Fatores principais na segurança de informática

Aula 03

Controle do acesso lógico às informações

- ter controle dos usuários X funções a serem executadas;
- Usuários não devem partilharem dos mesmos recursos sem que haja controle sobre o seu uso. Exemplo: o compartilhamento de chave de acesso por diversos usuários;
- Os microcomputadores sejam instalados em salas com controle no acesso de pessoas;
- O acesso a microcomputadores deve ser feito por meio de chaves de acesso autenticadas por senhas e controle sobre os domínios de recursos acessados.

Aula 03

Obscuridade das informações

Antes do advento dos computadores

- muitas informações eram registradas de formas “invisíveis” aos olhos humanos, a exemplo dos discos de vinil, fitas magnéticas e microfilmes.

Após o advento dos computadores

- o problema se tornou crucial. Devido ao fato de não serem “vistas” diretamente, tais informações são de controle mais difícil e podem ser mais facilmente roubadas ou fraudadas;
- a Internet aumenta ainda mais esse problema, já que na maioria dos acessos é impossível saber a origem das informações que estão sendo trazidas ao ambiente.

Aula 03

Segurança da Informação

Concentração de funções

Não surgiu com a informática. De certa forma a microinformática contribuiu para reduzir esse problema.

Motivo:

- Existência de maior número de profissionais com habilitação para executar as funções relacionadas com microcomputadores;
- Contribuição para disseminar as informações entre um maior número de ambientes informatizados.

Aula 03

Segurança da Informação

Falta de Controle

Não é decorrência da informática, embora ela torne o problema muito mais sério devido à velocidade com que as informações são processadas e acessadas em um ambiente informatizado.

A falta de controle pode implicar:

- a impossibilidade de descobrir irregularidades ou a descoberta somente após a ocorrência das mesmas;
- em microinformática – está intimamente associado com o problema do acesso indiscriminado;
- em relação a Internet – pode implicar em desvios de segurança que podem trazer conseqüências desastrosas

(ser atacados, grande parte com interesse no lucro financeiro que podem obter com suas informações).

Aula 03

Segurança da Informação

Retenção

A retenção da informação é um problema ainda mais grave em ambiente de microinformática do que em grandes computadores, pois é muito mais fácil carregar disquetes e CD's, e na maioria das organizações não existem controles sobre pacotes retirados das mesmas por funcionários e terceiros.

Informações armazenadas em meios de registros eletrônicos nem sempre são realmente apagadas quando se elimina o arquivo a elas associado. O que acontece na realidade é um mero cancelamento da referência de endereço do arquivo na tabela de conteúdo do meio de registro, com os dados permanecendo no espaço ocupado até que outro arquivo seja gravado em cima do mesmo espaço.

Aula 03

Segurança da Informação

Relacionamento e combinação de informações

Antes do advento da informática:

• Era muito mais difícil cruzar as informações de diversos arquivos para se obter uma nova informação.

Após o advento da informática:

• Com a utilização de banco de dados relacionais, tornou-se muito mais fácil, rápido – e pode levar à revelação de informações sigilosas ou até mesmo à invasão da privacidade das pessoas.

Internet → as informações não precisam estar armazenadas em um único local. Um atacante que conheça o perfil de seu negócio pode relacionar as informações que porventura consiga dentro de seu ambiente de informações com outras obtidas de outros ambientes.

Aula 03

Segurança da Informação

Introdução de erros

Existe um ditado em informática que diz:
"O lixo que entra é o lixo que sai ! "

Um erro introduzido em determinada fase do processamento, seja através de dados, de programas, se não descoberta a tempo pode se propagar rapidamente, tornando difícil e cara a sua eliminação.

Quanto mais aumenta a capacidade dos microcomputadores, mais grave se torna o problema da introdução de erros, podendo vir a atingir grandes proporções.

Na Internet existem pessoas cujo divertimento é simplesmente bagunçar as informações alheias.

Aula 03

Segurança da Informação

Lealdade

A lealdade é um problema muito sério em informática, devido à concentração de informações vitais em um único lugar.

A lealdade se torna um problema maior em ambientes de microinformática, pois muitos usuários acreditam ser os verdadeiros proprietários das aplicações que desenvolvem e, portanto, acham-se no direito de copiá-las e até vendê-las como se fossem suas.

O problema se complica em empresas com acesso externo a seus ambientes por meio de Internet. Funcionários desligados devem ter seus acessos à rede da empresa cancelados antes mesmo de deixarem o recinto da empresa pela última vez.

Aula 03

Segurança da Informação

Acesso não autorizado

Desde que os computadores começaram a ser usados, as tentativas de acesso não autorizados a eles existem e, para efeitos práticos, não se diferenciam do acesso indiscriminado.

Com o advento do processamento em tempo real, o problema tornou-se mais crítico, surgindo algumas formas de acesso não autorizado e abusos do direito de acesso.

Os grande computadores fazem uso de alguns tipos de monitoramento, são eles:
- Acesso de usuário finais – ferramenta de aplicações
- Acesso de serviços – ferramenta usada por profissionais de informática, que lhes permite acesso direto ao sistema operacional (é aqui que está o maior risco).

Aula 03

Segurança da Informação

Acesso não autorizado

Associados ao acesso não autorizado encontramos alguns termos destinados ao público especializado em informática. São:

- Hackers

São pessoas aficionadas por informática, normalmente com alto grau de inteligência e capacitação. Principal objetivo é ultrapassar barreiras de acesso aos grandes sistemas de computação que operam em rede, principalmente na Internet.

Em geral a atuação dos hackers não tem como finalidade a obtenção de vantagens econômicas para si, mas acabam por gerar inúmeros prejuízos sérios as organizações através de violação dos seus sistemas.

Diferenciando o conceito de Hacker e Cracker:
- Hacker seria aquele que viola para espionar sem destruir.
- Cracker, ao contrário, além de espionar, destrói ou altera a informação que encontra.

Aula 03

Segurança da Informação

Acesso não autorizado

- Vírus

Sua origem está relacionada pelas próprias empresas de software, que tinham a intenção de proteger seus produtos contra cópias não autorizadas.

Os vírus são raros em computadores de grande porte, ocorrendo com mais freqüência em microcomputadores e redes de computadores que estão conectadas entre si.

Podemos classificar como vírus, diversas formas de acesso não autorizado a sistemas que já existiam antes do advento da microinformática.

Vírus de computador é um nome genérico para programas que "infectam" seu computador, provocam algum efeito no funcionamento dele, e podem "contaminar" outros computadores através de disquetes, rede ou e-mail.

Aula 03

Segurança da Informação

Acesso não autorizado

- Bomba Lógica

É a forma de modificação não autorizada em sistemas mais difícil de ser detectada e a mais perigosa.

É também conhecida como bomba-relógio, pois na maioria dos casos o disparo é efetuado pela data do sistema, mas existem casos relacionados com os dados de entrada.

O principal fator envolvido é um funcionário com grande grau de conhecimento de informática e que, por um motivo qualquer, esteja descontente com a empresa.

Uma bomba lógica é o código que verifica se há determinadas circunstâncias e quando estas circunstâncias são encontradas, ele "detona" para fazer seus danos. Às vezes, como o vírus de Magellan, a lógica do disparador é uma data, mas pode ser dados outros parâmetros, incluindo o nome de uma pessoa, de um número de cliente do banco, ou de alguma combinação dos eventos e dos parâmetros.

Aula 03

Segurança da Informação

Acesso não autorizado

- Cavalo de Tróia (trojan horse)

Geralmente são feitos para rodarem em ambientes compartilhados. O programa assume o controle de um determinado terminal e exibe para os usuários uma máscara de tela igual à que apareceria normalmente, assim quando o usuário digitar o nome de seu usuário (login) e senha, o programa grava a informação e enviar para o hacker que fez o programa.

É um programa que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são:

- alteração ou destruição de arquivos;
- furto de senhas e outras informações sensíveis, como números de cartões de crédito;
- inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador.

Aula 03

Segurança da Informação

Acesso não autorizado

- Spyware, Keyloggers e hijackers

Apesar de não serem necessariamente vírus, estes três nomes também representam perigo. Spywares são programas que ficam "espionando" as atividades dos internautas ou capturam informações sobre eles. Para contaminar um computador, os spywares podem vir embutidos em softwares desconhecidos ou serem baixados automaticamente quando o internauta visita sites de conteúdo duvidoso.

Os keyloggers são pequenos aplicativos que podem vir embutidos em vírus, spywares ou softwares suspeitos, destinados a capturar tudo o que é digitado no teclado. O objetivo principal, nestes casos, é capturar senhas.

Hijackers são programas ou scripts que "seqüestram" 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, exibe propagandas em pop-ups ou janelas novas, instala barras de ferramentas no navegador e podem impedir acesso a determinados sites (como sites de software antivírus, por exemplo).

Obs.: No caso de hijackers, muitas vezes é necessário usar uma ferramenta desenvolvida especialmente para combater aquela praga. Isso porque os hijackers podem se infiltrar no sistema operacional de uma forma que nem antivírus nem anti-spywares conseguem "pegar".

Aula 03

Segurança da Informação

Acesso não autorizado

- Alçapão

Acesso ao sistema que de uma forma normal não seria permitido. Normalmente são programas que permanecem escondidos e somente serão usados quando necessários. Geralmente são desenvolvidos pelos próprios profissionais internos que, desta forma, querem manter uma via de acesso que contorne a segurança.

Aula 03

Segurança da Informação

Quebra de integridade

Como conseqüência do acesso não autorizado ou indiscriminado, uma empresa pode incorrer no risco de não ter como garantir a integridade das informações armazenadas em seus arquivos.

É necessário organização, definição e controle dos acessos e permissões aos usuários. Para que os mesmos possam realizar suas funções. Evitando permissões indiscriminadas e a quebra da integridade da informação.

Aula 03

Segurança da Informação

Técnicas de defesa

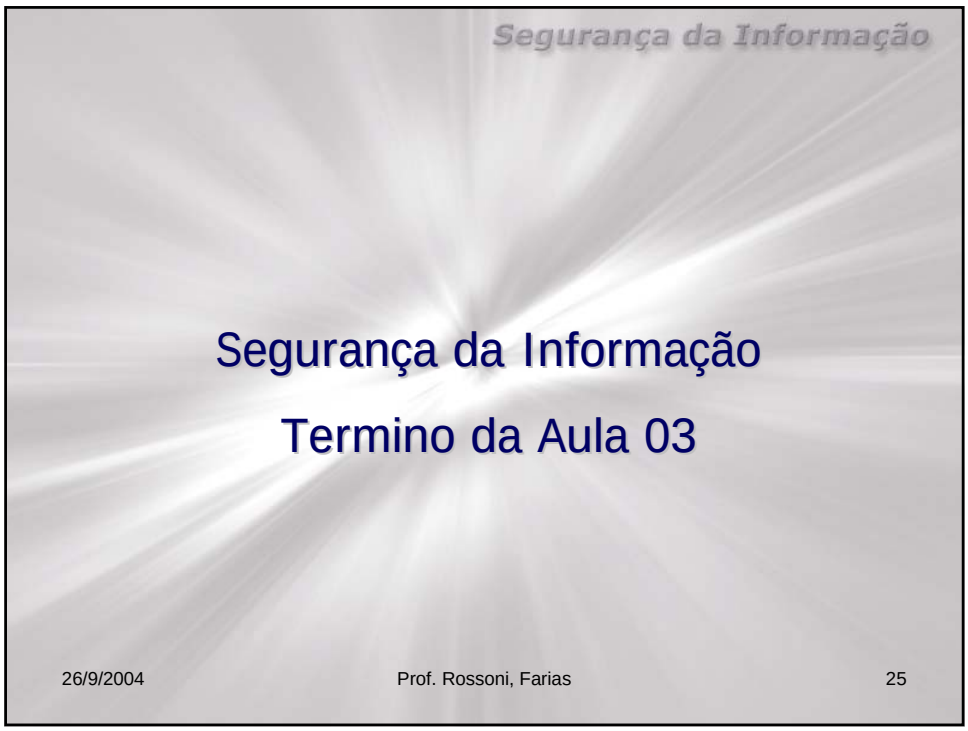
- Softwares de administração de redes;
- Softwares de segurança;
- Softwares de controle de oficialização de novos programas;
- Pacotes de administração de espaço em disco;
- Controle da fitoteca;
- Análise do sistema operacional;

Aula 03

Segurança da Informação

Técnicas de defesa – para pesquisas e combate a vírus

- Chaves de acessos individuais para cada funcionário autorizado a acessar facilidades computacionais, de modo que estabeleçam prontamente a cadeia de responsabilidades;
- Gravação de programas executáveis nas bibliotecas de programas, efetuado somente através de meio de acesso mantido sob estrito controle;
- Registro permanente e fiscalização das atividades executadas em cima de tais tipos de bibliotecas;
- Documentação organizada;
- Evitar ao máximo o acúmulo de responsabilidades e funções nas mãos de poucas pessoas.


Segurança da Informação
Segurança da Informação
Termino da Aula 03
26/9/2004
Prof. Rossoni, Farias
25