Segurança da Informação e Comunicação.
Princípios básicos; Dispositivos de armazenamentos de dados; Cópia de segurança (backup); Certificação e assinatura digital.

Conceitos de Proteção e Segurança da Informação e Comunicação

Segurança de Informação está relacionada com a proteção existente ou necessária sobre dados que possuem valor para alguém ou uma organização. Possui aspectos básicos como confidencialidade, integridade e disponibilidade da informação que nos ajuda a entender as necessidades de sua proteção e que não se aplica ou está restrita à sistemas computacionais, nem a informações eletrônicas ou qualquer outra forma mecânica de armazenamento. Ela se aplica a todos os aspectos de proteção e armazenamento de informações e dados, em qualquer forma. O nível de segurança de um sistema operacional de computador pode ser tipificado pela configuração de seus componentes.

Um dos padrões de segurança mais conhecidos é o BS7799, que estabelece melhores práticas para implementação e na gestão da segurança da informação.

Conceitos de segurança

A Segurança da Informação refere-se à proteção existente sobre as informações de uma determinada empresa, instituição governamental ou pessoa, isto é, aplica-se tanto as informações corporativas quanto as pessoais.

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente.

A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que tem o objetivo de furtar, destruir ou modificar a informação.

Antes de proteger, devemos saber:

- O que proteger.
- De quem proteger.
- Pontos vulneráveis.
- Processos a serem seguidos.

Ativo

Ativo é todo recurso que pode sofrer algum tipo de ataque, logo, precisa de proteção. Portanto todos os recursos que necessitam de alguma proteção, é considerado um ATIVO.

Avaliação – Colete informações suficientes para analisar o estado atual da Segurança no ambiente, e classificar quais bens estão protegidos. Com base nessa análise será possível classificar os ativos e ligá-los às suas respectivas ameaças.

Avaliar e Quantificar os Ativos

- **Avaliação e Quantificação dos recursos:** definir o valor das informações e dos serviços do ponto de vista dos terceiros envolvidos e do esforço necessário para recriar as informações. Baseado no custo da perda ou roubo de informação e/ou na queda de um serviço, podemos avaliar o custo deste recurso. O valor de um recurso deve refletir todos os custos identificados que poderiam surgir se houvesse algum problema com esse recurso.
- Defina a prioridade do recurso baseando-se na avaliação anterior e no custo monetário do recurso.

Prioridades do Ativo

- O servidor fornece funcionalidade básica, mas não tem impacto financeiro nos negócios.
- O servidor hospeda informações importantes, mas que podem ser recuperados rapidamente e com facilidade.
- O Servidor possui dados importantes e que demorariam muito tempo para serem recuperados.
- O servidor possui informações para os objetivos de negócio da empresa. A perda destas informações pode interromper projetos e o serviço diário de todos os usuários, o que causaria uma queda muito grande na produtividade da empresa.
- O servidor causa um grande impacto no negócio da empresa. A perda deste servidor ou a divulgação destas informações poderiam causar desvantagem competitiva da sua empresa. Veja o exemplo:

A tríade CIA (Confidentiality, Integrity and Availability) - Confidencialidade, Integridade e Disponibilidade - representa as principais propriedades que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja protejer.

Outras propriedades estão sendo apresentadas (legitimidade e autenticidade) na medida em que o uso de transações comerciais em todo o mundo, através de redes eletrônicas (públicas ou privadas) se desenvolve.

Os conceitos básicos podem ser explicados conforme abaixo:

- **A Disponibilidade:** o sistema deve estar disponível de forma que quando o usuário necessitar possa usar. Dados críticos devem estar disponíveis ininterruptamente.

Portanto, consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar. Isto pode ser chamado também de continuidade dos serviços.

- **A Utilização:** o sistema deve ser utilizado apenas para os determinados objetivos.

- **A Integridade:** o sistema deve estar sempre íntegro e em condições de ser usado.

A integridade consiste em proteger a informação contra modificação sem a permissão explícita do proprietário daquela informação. A modificação inclui ações como escrita, alteração de conteúdo, alteração de status, remoção e criação de informações. Deve-se considerar a proteção da informação nas suas mais variadas formas, como por exemplo, armazenada em discos ou fitas de backup. Integridade significa garantir que se o dado está lá, então não foi corrompido, encontra-se íntegro. Isto significa que aos dados originais nada foi acrescentado, retirado ou modificado. A integridade é assegurada evitando-se alteração não detectada de mensagens (ex. tráfego bancário) e o forjamento não detectado de mensagem (aliado à violação de autenticidade).

- **A Autenticidade:** o sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.

O controle de autenticidade está associado com identificação correta de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital. A verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema, de um sistema para o usuário ou de um sistema para outro sistema. Ela é a medida de proteção de um serviço/informação contra a personificação por intrusos.

- **A Confidencialidade:** dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele liberado. Significa proteger informações contra sua revelação para alguém não autorizado - interna ou externamente. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação deve ser protegida qualquer que seja a mídia que a

contenha, como por exemplo, mídia impressa ou mídia digital. Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso da rede, isto significa que os dados, enquanto em trânsito, não serão vistos, alterados, ou extraídos da rede por pessoas não autorizadas ou capturados por dispositivos ilícitos.

Para a montagem desta política, tem que se ter em conta:

- Riscos associados à falta de segurança;
- Benefícios;
- Custos de implementação dos mecanismos.

Mecanismos de segurança

O suporte para as recomendações de segurança pode ser encontrado em:

- **Controles físicos**: são barreiras que limitam o contato ou acesso direto a informação ou a infra-estrutura (que garante a existência da informação) que a suporta.

Devemos atentar para ameaças sempre presentes, mas nem sempre lembradas; incêndios, desabamentos, relâmpagos, alagamentos, problemas na rede elétrica, acesso indevido de pessoas aos servidores ou equipamentos de rede, treinamento inadequado de funcionários, etc.

Medidas de proteção física, tais como serviços de guarda, uso de no-breaks, alarmes e fechaduras, circuito interno de televisão e sistemas de escuta são realmente uma parte da segurança da informação. As medidas de proteção física são freqüentemente citadas como "segurança computacional", visto que têm um importante papel também na prevenção dos itens citados no parágrafo acima.

O ponto-chave é que as técnicas de proteção de dados por mais sofisticadas que sejam, não têm serventia nenhuma se a segurança física não for garantida.

Instalação e Atualização

A maioria dos sistemas operacionais, principalmente as distribuições Linux, vem acompanhada de muitos aplicativos que são instalados opcionalmente no processo de instalação do sistema. Sendo assim, torna-se necessário que vários pontos sejam observados para garantir a segurança desde a instalação do sistema, dos quais podemos destacar:

- **Seja minimalista:** Instale somente os aplicativos necessários, aplicativos com problemas podem facilitar o acesso de um atacante.
- **Devem ser desativados todos os serviços de sistema que não serão utilizados:** Muitas vezes o sistema inicia automaticamente diversos aplicativos que não são necessários, esses aplicativos também podem facilitar a vida de um atacante.
- **Deve-se tomar um grande cuidado com as aplicações de rede:** problemas nesse tipo de aplicação podem deixar o sistema vulnerável a ataques remotos que podem ser realizados através da rede ou Internet.
- **Use partições diferentes para os diferentes tipos de dados:** a divisão física dos dados facilita a manutenção da segurança.
- **Remova todas as contas de usuários não utilizadas:** Contas de usuários sem senha, ou com a senha original de instalação, podem ser facilmente exploradas para obter-se acesso ao sistema.

De acordo com diversos anúncios publicados pelo CERT (2000:web), grande parte das invasões na Internet acontece devido à falhas conhecidas em aplicações de rede, as quais os administradores de sistemas não foram capazes de corrigir a tempo. Essa afirmação pode ser confirmada facilmente pelo simples fato de que quando uma nova vulnerabilidade é descoberta, um grande número de ataques é realizado com sucesso. Por isso é extremamente importante que os administradores de sistemas se mantenham atualizados sobre os principais problemas encontrados nos aplicativos utilizados, através dos sites dos desenvolvedores ou específicos sobre segurança da Informação. As principais empresas comerciais

desenvolvedoras de software e as principais distribuições Linux possuem boletins periódicos informando sobre as últimas vulnerabilidades encontradas e suas devidas correções. Alguns sistemas chegam até a possuir o recurso de atualização automática, facilitando ainda mais o processo.

Desenvolvimento Seguro de Aplicações WEB

O desenvolvimento de aplicações que irão utilizar a internet como interface, designadas aqui como Aplicações WEB, exige uma maior preocupação com a segurança no processamento e armazenamento dos dados. Esse tipo de aplicação fica exposta um grande número de usuários e ameaças. Hackers estão constantemente testando as
aplicações em busca de vulnerabilidades que possam facilitar o acesso a um sistema, ou simplesmente falhas que possam negar um serviço, como nos ataques DoS ou DDoS.

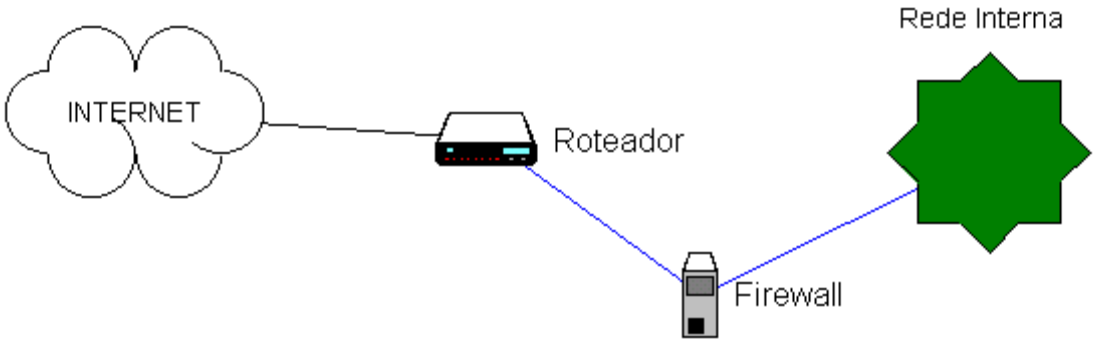
Sendo assim, podemos destacar algumas das principais práticas para o desenvolvimento seguro de aplicações WEB:

- **Não use mais poder do que o necessário:** As aplicações devem rodar num nível de acesso suficiente para utilizar somente os recursos necessários do servidor, não em níveis superiores, pois em caso de falhas na aplicação, ela somente terá acesso aos seus recursos e não aos pertencentes a outros processos.
- **Não use o método GET para mandar informações sensíveis:** O método GET é um mecanismo para passagens de parâmetro entre páginas WEB, as informações transmitidas podem ser facilmente capturadas, sendo que muitas vezes nem o protocolo SSL pode solucionar esse problema.
- **Nunca confie nas informações fornecidas pelo usuário:** As aplicações sempre devem validar as informações enviadas pelo usuário, verificando o formato e tamanho dos dados para evitar possíveis Buffers Overflows ou outros problemas.
- **Não guarde as senhas de acesso ao banco de dados ou outros recursos dentro de páginas pré-processadas ou scripts cgi:** Muitas vezes é possível obter o seu código fonte, obtendo-se assim senhas e outras informações sensíveis.
- **Use criptografia para armazenar informações sensíveis no servidor:** Dessa maneira é possível proteger números de cartão de crédito em sites de comércio eletrônico, ou qualquer outra informação importante**.**
- **Procure não utilizar programas externos à linguagem:** Em alguns casos é mais fácil utilizar chamadas a programas executáveis diretamente no sistema operacional em vez de implementar um procedimento num programa. Esse tipo de ação acaba por expor o aplicativo à falhas de segurança de outros aplicativos, como também a problemas de validação que possam permitir a execução remota de comandos.
- **Não deixe comentário no código de produção:** Caso possam ser visualizados eles podem auxiliar muito o trabalho de algum invasor.
- **Verifique e personalize as mensagens de erro:** Muitas vezes as mensagens de erro padrão de uma linguagem podem fornecer informações valiosas sobre o servidor.
- **Utilize ferramentas, linguagens e bibliotecas atualizadas:** Caso elas possuam algum problema de segurança todo o sistema estará comprometido.

Firewalls

Definimos o firewall como sendo uma barreira inteligente entre duas redes, geralmente a rede local e a Internet, através da qual só passa tráfego autorizado. Este tráfego é examinado pelo firewall em tempo real e a seleção é feita de acordo com um conjunto de regras de acesso Ele é tipicamente um roteador (equipamento que liga as redes com a Internet), um computador rodando filtragens de pacotes, um software proxy, um firewall-in-a-box (um hardware proprietário específico para função de firewall), ou um conjunto desses sistemas.

Pode-se dizer que firewall é um conceito ao invés de um produto. Ele é a soma de todas as regras aplicadas a rede. Geralmente, essas regras são elaboradas considerando as políticas de acesso da organização.
A figura abaixo, descreve o modelo mais comumente utilizado para implementação de um firewall:



Podemos observar que o firewall é único ponto de entrada da rede, quando isso acontece o firewall também pode ser designado como chock point.
De acordo com os mecanismos de funcionamentos dos firewalls podemos destacar três tipos principais:

- Filtros de pacotes
- Stateful Firewalls
- Firewalls em Nível de Aplicação

Filtros de Pacotes

Esse é o tipo de firewall mais conhecido e utilizado. Ele controla a origem e o destino dos pacotes de mensagens da Internet. Quando uma informação é recebida, o firewall verifica as informações sobre o endereço IP de origem e destino do pacote e compara com uma lista de regras de acesso para determinar se pacote está autorizado ou não a ser repassado através dele.

Atualmente, a filtragem de pacotes é implementada na maioria dos roteadores e é transparente aos usuários, porém pode ser facilmente contornada com IP Spoofers. Por isto, o uso de roteadores como única defesa para uma rede corporativa não é aconselhável.
Mesmo que filtragem de pacotes possa ser feita diretamente no roteador, para uma maior performance e controle, é necessária a utilização de um sistema específico de firewall. Quando um grande número de regras é aplicado diretamente no roteador, ele acaba perdendo performance. Além disso, Firewall mais avançados podem defender a rede contra spoofing e ataques do tipo DoS/DDoS.

Stateful Firewalls

Um outro tipo de firewall é conhecido como Stateful Firewall. Ele utiliza uma técnica chamada Stateful Packet Inspection, que é um tipo avançado de filtragem de pacotes. Esse tipo de firewall examina todo o conteúdo de um pacote, não apenas seu cabeçalho, que contém apenas os endereços de origem e destino da informação. Ele é chamado de 'stateful' porque examina os conteúdos dos pacotes para determinar qual é o estado da conexão, **Ex**: Ele garante que o computador destino de uma informação tenha realmente solicitado anteriormente a informação através da conexão atual.
Além de serem mais rigorosos na inspeção dos pacotes, os stateful firewalls podem ainda manter as portas fechadas até que uma conexão para a porta específica seja requisitada. Isso permite uma maior proteção contra a ameaça de port scanning.

Firewalls em Nível de Aplicação

Nesse tipo de firewall o controle é executado por aplicações específicas, denominadas proxies, para cada tipo de serviço a ser controlado. Essas aplicações interceptam todo o tráfego recebido e o envia para as aplicações correspondentes; assim, cada aplicação pode controlar o uso de um serviço.

Apesar desse tipo de firewall ter uma perda maior de performance, já que ele analisa toda a comunicação utilizando proxies, ele permite uma maior auditoria sobre o controle no tráfego, já que as aplicações específicas podem detalhar melhor os eventos associados a um dado serviço.
A maior dificuldade na sua implementação é a necessidade de instalação e configuração de um proxy para cada aplicação, sendo que algumas aplicações não trabalham corretamente com esses mecanismos.

Considerações sobre o uso de Firewalls

Embora os firewalls garantam uma maior proteção, e são inestimáveis para segurança da informação, existem alguns ataques que os firewalls não podem proteger, como a interceptação de tráfego não criptografado, ex: Interceptação de e-mail. Além disso, embora os firewalls possam prover um único ponto de segurança e auditoria, eles também podem se tornar um único ponto de falha – o que quer dizer que os firewalls são a última linha de defesa. Significa que se um atacante conseguir quebrar a segurança de um firewall, ele vai ter acesso ao sistema, e pode ter a oportunidade de roubar ou destruir informações. Além disso, os firewalls protegem a rede contra os ataques externos, mas não contra os ataques internos. No caso de funcionários mal intencionados, os firewalls não garantem muita proteção. Finalmente, como mencionado os firewalls de filtros de pacotes são falhos em alguns pontos. - As técnicas de Spoofing podem ser um meio efetivo de anular a sua proteção.

Para uma proteção eficiente contra as ameaças de segurança existentes, os firewalls devem ser usados em conjunto com diversas outras medidas de segurança.

Existem, claro, outros mecanismos de segurança que apóiam os controles físicos: Portas / trancas / paredes / blindagem / guardas / etc ..

- **Controles lógicos: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.**

Existem mecanismos de segurança que apóiam os controles lógicos:

Mecanismos de encriptação. A criptografia vem, na sua origem, da fusão de duas palavras gregas:

- CRIPTO = ocultar, esconder
- GRAFIA = escrever

Criptografia é arte ou ciência de escrever em cifra ou em códigos. É então um conjunto de técnicas que tornam uma mensagem incompreensível permitindo apenas que o destinatário que conheça a chave de encriptação possa decriptar e ler a mensagem com clareza.
Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não encriptados, produzir uma sequência de dados encriptados. A operação inversa é a desencriptação.

Assinatura digital. Um conjunto de dados encriptados, associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade.

A assinatura digital, portanto, busca resolver dois problemas não garantidos apenas com uso da criptografia para codificar as informações: a Integridade e a Procedência.
Ela utiliza uma função chamada one-way hash function, também conhecida como: compression function, cryptographic checksum, message digest ou fingerprint. Essa função gera uma string única sobre uma informação, se esse valor for o mesmo tanto no remetente quanto destinatário, significa que essa informação não foi alterada.
Mesmo assim isso ainda não garante total integridade, pois a informação pode ter sido alterada no seu envio e um novo hash pode ter sido calculado.

Para solucionar esse problema, é utilizada a criptografia assimétrica com a função das chaves num sentido inverso, onde o hash é criptografado usando a chave privada do remetente, sendo assim o destinatário de posse da chave pública do remetente poderá decriptar o hash. Dessa maneira garantimos a procedência, pois somente o remetente possui a chave privada para codificar o hash que será aberto pela sua chave pública. Já o hash, gerado a partir da informação original, protegido pela criptografia, garantirá a integridade da informação.

Mecanismos de garantia da integridade da informação. Usando funções de "Hashing" ou de checagem, consistindo na adição.

***Mecanismos de controle de acesso*.** Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.

Mecanismos de certificação. Atesta a validade de um documento. O Certificado Digital, também conhecido como Certificado de Identidade Digital, associa a identidade de um titular a um par de chaves eletrônicas (uma pública e outra privada) que, usadas em conjunto, fornecem a comprovação da identidade. É uma versão eletrônica (digital) de algo parecido a uma Cédula de Identidade - serve como prova de identidade, reconhecida diante de qualquer situação onde seja necessária a comprovação de identidade.

O Certificado Digital pode ser usado em uma grande variedade de aplicações, como comércio eletrônico, groupware (Intranet's e Internet) e transferência eletrônica de fundos.

Dessa forma, um cliente que compre em um shopping virtual, utilizando um Servidor Seguro, solicitará o Certificado de Identidade Digital deste Servidor para verificar: a identidade do vendedor e o conteúdo do Certificado por ele apresentado. Da mesma forma, o servidor poderá solicitar ao comprador seu Certificado de Identidade Digital, para identificá-lo com segurança e precisão.
Caso qualquer um dos dois apresente um Certificado de Identidade Digital adulterado, ele será avisado do fato, e a comunicação com segurança não será estabelecida.

O Certificado de Identidade Digital é emitido e assinado por uma Autoridade Certificadora Digital (Certificate Authority). Para tanto, esta autoridade usa as mais avançadas técnicas de criptografia disponíveis e de padrões internacionais (norma ISO X.509 para Certificados Digitais), para a emissão e chancela digital dos Certificados de Identidade Digital.

Podemos destacar três elementos principais:
Informação de atributo: É a informação sobre o objeto que é certificado. No caso de uma pessoa, isto pode incluir seu nome, nacionalidade e endereço e-mail, sua organização e o departamento da organização onde trabalha.

Chave de informação pública: É a chave pública da entidade certificada. O certificado atua para associar a chave pública à informação de atributo, descrita acima. A chave pública pode ser qualquer chave assimétrica, mas usualmente é uma chave RSA.

Assinatura da Autoridade em Certificação (CA): A CA assina os dois primeiros elementos e, então, adiciona credibilidade ao certificado. Quem recebe o certificado verifica a assinatura e acreditará na informação de atributo e chave pública associadas se acreditar na Autoridade em Certificação.

Existem diversos protocolos que usam os certificados digitais para comunicações seguras na Internet:

- Secure Socket Layer ou SSL
- Secured Multipurpose Mail Extensions - S/MIME
- Form Signing
- Authenticode / Objectsigning

O SSL é talvez a mais difundida aplicação para os certificados digitais e é usado em praticamente todos os sites que fazem comércio eletrônico na rede (livrarias, lojas de CD, bancos etc.). O SSL teve uma primeira fase de adoção onde apenas os servidores estavam

identificados com certificados digitais, e assim tínhamos garantido, além da identidade do servidor, o sigilo na sessão. Entretanto, apenas com a chegada dos certificados para os browsers é que pudemos contar também com a identificação na ponta cliente, eliminando assim a necessidade do uso de senhas e logins.

O S/Mime é também um protocolo muito popular, pois permite que as mensagens de correio eletrônico trafeguem encriptadas e/ou assinadas digitalmente. Desta forma os e-mails não podem ser lidos ou adulterados por terceiros durante o seu trânsito entre a máquina do remetente e a do destinatário. Além disso, o destinatário tem a garantia da identidade de quem enviou o e-mail.

O Form Signing é uma tecnologia que permite que os usuários emitam recibos online com seus certificados digitais. Por exemplo: o usuário acessa o seu Internet Banking e solicita uma transferência de fundos. O sistema do banco, antes de fazer a operação, pede que o usuário assine com seu certificado digital um recibo confirmando a operação. Esse recibo pode ser guardado pelo banco para servir como prova, caso o cliente posteriormente negue ter efetuado a transação.

O Authenticode e o Object Signing são tecnologias que permitem que um desenvolvedor de programas de computador assine digitalmente seu software. Assim, ao baixar um software pela Internet, o usuário tem certeza da identidade do fabricante do programa e que o software se manteve íntegro durante o processo de download. Os certificados digitais se dividem em basicamente dois formatos: os certificados de uso geral (que seriam equivalentes a uma carteira de identidade) e os de uso restrito (equivalentes a cartões de banco, carteiras de clube etc.). Os certificados de uso geral são emitidos diretamente para o usuário final, enquanto que os de uso restrito são voltados basicamente para empresas ou governo.

Integridade. Medida em que um serviço/informação é genuino, isto é, esta protegido contra a personificação por intrusos.

Honeypot: É o nome dado a um software, cuja função é detectar ou de impedir a ação de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.

Ameaças à segurança

Ameaça é algo que oferece um risco e tem como foco algum ativo. Uma ameaça também pode aproveitar-se de alguma vulnerabilidade do ambiente.

Identificar Ameaças de Segurança – Identificar os Tipos de Ataques é a base para chegar aos Riscos. Lembre-se que existem as prioridades; essas prioridades são os pontos que podem comprometer o “Negócio da Empresa”, ou seja, o que é crucial para a sobrevivência da Empresa é crucial no seu projeto de Segurança.

Abaixo temos um conjunto de ameaças, chamado de FVRDNE:

Falsificação
Falsificação de Identidade é quando se usa nome de usuário e senha de outra pessoa para acessar recursos ou executar tarefas. Seguem dois exemplos:
- Falsificar mensagem de e-mail
- Executar pacotes de autenticação

Um ataque de Falsificação pode ter início em um PostIt com sua senha, grudado no seu monitor.

Violação
A Violação ocorre quando os dados são alterados:
- Alterar dados durante a transmissão
- Alterar dados em arquivos

Repudiação
A Repudiação talvez seja uma das últimas etapas de um ataque bem sucedido, pois é o ato de negar algo que foi feito. Isso pode ser feito apagando as entradas do Log após um acesso indevido. Exemplos:
- Excluir um arquivo crítico e negar que excluiu
- Comprar um produto e mais tarde negar que comprou

Divulgação
A Divulgação das Informações pode ser tão grave e/ou custar tão caro quanto um ataque de "Negação de Serviço", pois informações que não podiam ser acessadas por terceiros, agora estão sendo divulgadas ou usadas para obter vantagem em negócios.
Dependendo da informação ela pode ser usada como objeto de chantagem. Abaixo exemplos de Divulgação:
- Expor informações em mensagens de erro
- Expor código em sites

Negação de Serviço (DoS) *(*Denial of Service*, DoS)*:
A forma mais conhecida de ataque que consiste na perturbação de um serviço, devido a danos físicos ou lógicos causados no sistema que o suportam. Para provocar um DoS, os atacantes disseminam vírus, geram grandes volumes de tráfego de forma artificial, ou muitos pedidos aos servidores que causam subcarga e estes últimos ficam impedidos de processar os pedidos normais.
O objetivo deste ataque é parar algum serviço. Exemplo:
- "Inundar" uma rede com pacotes SYN (Syn-Flood)
- "Inundar" uma rede com pacotes ICPM forçados

O alvo deste tipo de ataque pode ser um Web Server contendo o site da empresa, ou até mesmo "inundar" o DHCP Server Local com solicitações de IP, fazendo com que nenhuma estação com IP dinâmico obtenha endereço IP.

Elevação de Privilégios
Acontece quando o usuário mal-intencionado quer executar uma ação da qual não possui privilégios administrativos suficientes:
- Explorar saturações do buffer para obter privilégios do sistema
- Obter privilégios de administrador de forma ilegítima

Este usuário pode aproveitar-se que o Administrador da Rede efetuou logon numa máquina e a deixou desbloqueada, e com isso adicionar a sua própria conta aos grupos Domain Admins, e Remote Desktop Users. Com isso ele faz o que quiser com a rede da empresa, mesmo que esteja em casa.

Quem pode ser uma ameaça?

Quem ataca a rede/sistema são agentes maliciosos, muitas vezes conhecidos como **crackers**, (**hackers** não são agentes maliciosos, tentam ajudar a encontrar possíveis falhas). Estas pessoas são motivadas para fazer esta ilegalidade por vários motivos. Os principais motivos são: notoriedade, auto-estima, vingança e o dinheiro. É sabido que mais de 70% dos ataques partem de usuários legítimos de sistemas de informação (Insiders) -- o que motiva corporações a investir largamente em controles de segurança para seus ambientes corporativos (intranet).

É necessário identificar quem pode atacar a minha rede, e qual a capacidade e/ou objetivo desta pessoa.
- **Principiante –** não tem nenhuma experiência em programação e usa ferramentas de terceiros. Geralmente não tem noção do que está fazendo ou das conseqüências daquele ato**.**
- **Intermediário –** tem algum conhecimento de programação e utiliza ferramentas usadas por terceiros. Esta pessoa pode querer algo além de testar um "Programinha Hacker".
- **Avançado –** Programadores experientes, possuem conhecimento de Infra-Estrutura e Protocolos. Podem realizar ataques estruturados. Certamente não estão só testando os seus programas.

Estas duas primeiras pessoas podem ser funcionários da empresa, e provavelmente estão se aproveitando de alguma vulnerabilidade do seu ambiente.

Vulnerabilidades

Os ataques com mais chances de dar certo são aqueles que exploram vulnerabilidades, seja ela uma vulnerabilidade do sistema operacional, aplicativos ou políticas internas.

Veja algumas vulnerabilidades:

- **Roubo de senhas –** Uso de senhas em branco, senhas previsíveis ou que não usam requisitos mínimos de complexidade. Deixar um Postit com a sua senha grudada no monitor é uma vulnerabilidade.
- **Software sem Patches –** Um gerenciamento de Service Packs e HotFixes mal feito é uma vulnerabilidade comum. Veja casos como os ataques do Slammer e do Blaster, sendo que suas respectivas correções já estavam disponíveis bem antes dos ataques serem realizados.
- **Configuração Incorreta –** Aplicativos executados com contas de Sistema Local, e usuários que possuem permissões acima do necessário.
- **Engenharia Social –** O Administrador pode alterar uma senha sem verificar a identidade da chamada.
- **Segurança fraca no Perímetro –** Serviços desnecessários, portas não seguras. Firewall e Roteadores usadas incorretamente.
- **Transporte de Dados sem Criptografia –** Pacotes de autenticação usando protocolos de texto simples, dados importantes enviados em texto simples pela Internet.

Identifique, entenda como explorá-las e mesmo que não seja possível eliminá-las, monitore e gerencie o risco de suas vulnerabilidades.

Nem todos os problemas de segurança possuem uma solução definitiva, a partir disso inicia-se o Gerenciamento de Risco, analisando e balanceando todas as informações sobre Ativos, Ameaças, Vulnerabilidades, probabilidade e impacto.

Nível de segurança

Depois de identificado o potencial de ataque, as organizações têm que decidir o nível de segurança a estabelecer para um rede ou sistema os recursos físicos e lógicos a necessitar de proteção. No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de proteção para minimizar a probabilidade de ocorrência de um ataque .

Políticas de segurança

De acordo com o RFC 2196 (*The Site Security Handbook*), uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos usuários dos recursos de uma organização.

As políticas de segurança deve ter implementação realista, e definir claramente as áreas de responsabilidade dos usuários, do pessoal de gestão de sistemas e redes e da direção. Deve também adaptar-se a alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

O documento que define a política de segurança deve deixar de fora todos os aspetos técnicos de implementação dos mercanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

Algumas normas definem aspectos que devem ser levados em consideração ao elaborar políticas de segurança. Entre essas normas estão a BS 7799 (elaborada pela British Standards Institution) e a NBR ISO/IEC 17799 (a versão brasileira desta primeira).

Existem duas filosofias por trás de qualquer política de segurança: **a proibitiva** (tudo que não é expressamente permitido é proibido) e a **permissiva** (tudo que não é proibido é permitido).

Enfim, implantar Segurança em um ambiente não depende só da Tecnologia usada, mas também dos Processos utilizados na sua implementação e da responsabilidade que as Pessoas têm neste conjunto. Estar atento ao surgimento de novas tecnologias não basta, é necessário entender as necessidades do ambiente, e implantar políticas que conscientizem as pessoas a trabalhar de modo seguro.

Seu ambiente nunca estará seguro, não imagine que instalando um bom Antivírus você elimina as suas vulnerabilidades ou diminui a quantidade de ameaças. É extremamente necessário conhecer o ambiente e fazer um estudo, para depois poder implementar ferramentas e soluções de segurança.

NOÇÕES BÁSICAS A RESPEITO DE VÍRUS DE COMPUTADOR

DEFINIÇÃO E PROGRAMAS ANTIVÍRUS

O que são vírus de computador?

Os vírus representam um dos maiores problemas para usuários de computador.
Consistem em pequenos programas criados para causar algum dano ao computador infectado, seja apagando dados, seja capturando informações, seja alterando o funcionamento normal da máquina. Os usuários dos sistemas operacionais Windows são vítimas quase que exclusivas de vírus, já que os sistemas da Microsoft são largamente usados no mundo todo. Existem vírus para sistemas operacionais Mac e os baseados em Unix, mas estes são extremamente raros e costumam ser bastante limitados. Esses "*programas maliciosos*" receberam o nome vírus porque possuem a característica de se multiplicar facilmente, assim como ocorre com os vírus reais, ou seja, os vírus biológicos. Eles se disseminam ou agem por meio de falhas ou limitações de determinados programas, se espalhando como em uma infecção.

Para contaminarem os computadores, os vírus antigamente usavam disquetes ou arquivos infectados. Hoje, os vírus podem atingir em poucos minutos milhares de computadores em todo mundo. Isso tudo graças à *Internet*. O método de propagação mais comum é o uso de *e-mails*, onde o vírus usa um texto que tenta convencer o internauta a clicar no arquivo em anexo. É nesse anexo que se encontra o vírus. Os meios de convencimento são muitos e costumam ser bastante criativos. O e-mail (e até o campo assunto da mensagem) costuma ter textos que despertam a curiosidade do internauta. Muitos exploram assuntos eróticos ou abordam questões atuais. Alguns vírus podem até usar um remetente falso, fazendo o destinatário do e-mail acreditar que trata-se de uma mensagem verdadeira. Muitos internautas costumam identificar e-mails de vírus, mas os criadores destas "*pragas digitais*" podem usar artifícios inéditos que não poupam nem o usuário mais experiente.

O computador (ou, melhor dizendo, o sistema operacional), por si só, não tem como detectar a existência deste programinha. Ele não é referenciado em nenhuma parte dos seus arquivos, ninguém sabe dele, e ele não costuma se mostrar antes do ataque fatal.
Em linhas gerais, um vírus completo (entenda-se por completo o vírus que usa todas as formas possíveis de contaminar e se ocultar) chega até a memória do computador de duas formas.

A primeira e a mais simples é a seguinte: em qualquer disco (tanto disquete quanto HD) existe um setor que é lido primeiro pelo sistema operacional quando o computador o acessa. Este setor identifica o disco e informa como o sistema operacional (SO) deve agir. O vírus se aloja exatamente neste setor, e espera que o computador o acesse.

A partir daí ele passa para a memória do computador e entra na segunda fase da infecção. Mas antes de falarmos da segunda fase, vamos analisar o segundo método de infecção: o vírus se agrega a um arquivo executável (fica pendurado mesmo nesse arquivo). Acessar o disco onde este arquivo está não é o suficiente para se contaminar.

É preciso executar o arquivo contaminado. O vírus se anexa, geralmente, em uma parte do arquivo onde não interfira no seu funcionamento (do arquivo), pois assim o usuário não vai perceber nenhuma alteração e vai continuar usando o programa infectado.

O vírus, após ter sido executado, fica escondido agora na memória do computador, e imediatamente infecta todos os discos que estão ligados ao computador, colocando uma cópia de si mesmo no tal setor que é lido primeiro (chamado setor de boot), e quando o disco for transferido para outro computador, este ao acessar o disco contaminado (lendo o setor de boot), executará o vírus e o alocará na sua memória, o que por sua vez irá infectar todos os discos utilizados neste computador, e assim o vírus vai se alastrando.

Os vírus que se anexam a arquivos infectam também todos os arquivos que estão sendo ou e serão executados. Alguns às vezes re-contaminam o mesmo arquivo tantas vezes e ele fica tão grande que passa a ocupar um espaço considerável (que é sempre muito precioso) em seu disco. Outros, mais inteligentes, se escondem entre os espaços do programa original, para não dar a menor pista de sua existência.

Cada vírus possui um critério para começar o ataque propriamente dito, onde os arquivos começam a ser apagados, o micro começa a travar, documentos que não são salvos e várias outras tragédias. Alguns apenas mostram mensagens chatas, outros mais elaborados fazem estragos muitos grandes.

Tipos

Cavalo-de-tróia

A denominação “Cavalo de Tróia” (Trojan Horse) foi atribuída aos programas que permitem a invasão de um computador alheio com espantosa facilidade. Nesse caso, o termo é análogo ao famoso artefato militar fabricado pelos gregos espartanos. Um “amigo” virtual presenteia o outro com um “presente de grego”, que seria um aplicativo qualquer. Quando o leigo o executa, o programa atua de forma diferente do que era esperado.

Ao contrário do que é erroneamente informado na mídia, que classifica o Cavalo de Tróia como um vírus, ele não se reproduz e não tem nenhuma comparação com vírus de computador, sendo que seu objetivo é totalmente diverso. Deve-se levar em consideração, também, que a maioria dos antivírus fazem a sua detecção e os classificam como tal. A expressão “Trojan” deve ser usada, exclusivamente, como definição para programas que capturam dados sem o conhecimento do usuário.

O Cavalo de Tróia é um programa que se aloca como um arquivo no computador da vítima. Ele tem o intuito de roubar informações como passwords, logins e quaisquer dados, sigilosos ou não, mantidos no micro da vítima. Quando a máquina contaminada por um Trojan conectar-se à Internet, poderá ter todas as informações contidas no HD visualizadas e capturadas por um intruso qualquer. Estas visitas são feitas imperceptivelmente. Só quem já esteve dentro de um computador alheio sabe as possibilidades oferecidas.

Worm

Os worms (vermes) podem ser interpretados como um tipo de vírus mais inteligente que os demais. A principal diferença entre eles está na forma de propagação: os worms podem se propagar rapidamente para outros computadores, seja pela Internet, seja por meio de uma rede local. Geralmente, a contaminação ocorre de maneira discreta e o usuário só nota o problema quando o computador apresenta alguma anormalidade. O que faz destes vírus inteligentesé a gama de possibilidades de propagação. O worm pode capturar endereços de e-mail em arquivos do usuário, usar serviços de SMTP (sistema de envio de e-mails) próprios ou qualquer outro meio que permita a contaminação de computadores (normalmente milhares) em pouco tempo.

Spywares, 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 "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, 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).

Os spywares e os keyloggers podem ser identificados por programas anti-spywares. Porém, algumas destas pragas são tão perigosas que alguns antivírus podem ser preparados para identificá-las, como se fossem vírus. 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".

Hoaxes, o que são?

São boatos espalhados por mensagens de correio eletrônico, que servem para assustar o usuário de computador. Uma mensagem no e-mail alerta para um novo vírus totalmente destrutivo que está circulando na rede e que infectará o micro do destinatário enquanto a mensagem estiver sendo lida ou quando o usuário clicar em determinada tecla ou link. Quem cria a mensagem hoax normalmente costuma dizer que a informação partiu de uma empresa confiável, como IBM e Microsoft, e que tal vírus poderá danificar a máquina do usuário. Desconsidere a mensagem.

Firewall

Firewall é um programa que monitora as conexões feitas pelo seu computador para garantir que nenhum recurso do seu computador esteja sendo usado indevidamente. São úteis para a prevenção de worms e trojans.

Antivírus

Existe uma variedade enorme de softwares antivírus no mercado. Independente de qual você usa, mantenha-o sempre atualizado. Isso porque surgem vírus novos todos os dias e seu antivírus precisa saber da existência deles para proteger seu sistema operacional.

A maioria dos softwares antivírus possuem serviços de atualização automática. Abaixo há uma lista com os antivírus mais conhecidos:

Norton AntiVirus - Symantec - www.symantec.com.br - Possui versão de teste.

McAfee - McAfee - http://www.mcafee.com.br - Possui versão de teste.

AVG - Grisoft - www.grisoft.com - Possui versão paga e outra gratuita para uso não-comercial (com menos funcionalidades).

Panda Antivirus - Panda Software - www.pandasoftware.com.br - Possui versão de teste.

É importante frisar que a maioria destes desenvolvedores possuem ferramentas gratuitas destinadas a remover vírus específicos. Geralmente, tais softwares são criados para combater vírus perigosos ou com alto grau de propagação.

Proteção

A melhor política com relação à proteção do seu computador contra vírus é *possuir um bom software anti-vírus original instalado e atualizá-lo com freqüência,* pois surgem vírus novos a cada dia. Portanto, a regra básica com relação a vírus (e outras infecções) é*:* ***Jamais execute programas que não tenham sido obtidos de fontes absolutamente confiáveis.*** O tema dos vírus é muito extenso e não se pode pretender abordá-lo aqui senão superficialmente, para dar orientações essenciais. Vamos a algumas recomendações.

Os processos mais comuns de se receber arquivos são como anexos de mensagens de e-mail, através de programas de FTP, ou por meio de programas de comunicação, como o ICQ, o NetMeeting, etc.

Note que:

Não existem vírus de e-mail. O que existem são vírus escondidos em programas anexados ao e-mail. Você não infecta seu computador só de ler uma mensagem de correio eletrônico escrita em formato texto (.txt). Mas evite ler o conteúdo de arquivos anexados sem antes certificar-se de que eles estão livres de vírus. Salve-os em um diretório e passe um programa antivírus atualizado. Só depois abra o arquivo.

Cuidados que se deve tomar com mensagens de correio eletrônico – Como já foi falado, simplesmente ler a mensagem não causa qualquer problema. No entanto, se a mensagem contém anexos (ou attachments, em Inglês), é preciso cuidado. O anexo pode ser um arquivo executável (programa) e, portanto, pode estar contaminado. A não ser que você tenha certeza absoluta da integridade do arquivo, é melhor ser precavido e suspeitar. Não abra o arquivo sem antes passá-lo por uma análise do anti-vírus atualizado

Mas se o anexo não for um programa, for um arquivo apenas de texto, é possível relaxar os cuidados?
Não. Infelizmente, os criadores de vírus são muito ativos, e existem hoje, disseminando-se rapidamente, vírus que contaminam arquivos do MS Word ou do MS Excel. São os chamados vírus de macro, que infectam as macros (executáveis) destes arquivos. Assim, não abra anexos deste tipo sem prévia verificação.

É possível clicar no indicador de anexo para ver do que se trata? E como fazer em seguida?

Apenas clicar no indicador (que no MS Outlook Express é uma imagem de um clip), sim. Mas cuidado para não dar um clique duplo, ou clicar no nome do arquivo, pois se o anexo for um programa, será executado. Faça assim:

1- Abra a janela da mensagem (em que o anexo aparece como um ícone no rodapé);

2- Salve o anexo em um diretório à sua escolha, o que pode ser feito de dois modos

a) clicar o anexo com o botão direito do mouse e em seguida clicar em "Salvar como...";

b) seqüência de comandos: Arquivo / Salvar anexos...

3- Passe um *anti-vírus atualizado* no anexo salvo para se certificar de que este não está infectado.

Riscos dos "download"- Simplesmente baixar o programa para o seu computador não causa infecção, seja por FTP, ICQ, ou o que for. Mas de modo algum execute o programa (de qualquer tipo, joguinhos, utilitários, protetores de tela, etc.) sem antes submetê-lo a um bom anti-vírus.

O que acontece se ocorrer uma infecção?
Você ficará à mercê de pessoas inescrupulosas quando estiver conectado à Internet. Elas

poderão invadir seu computador e realizar atividades nocivas desde apenas ler seus arquivos, até causar danos como apagar arquivos, e até mesmo roubar suas senhas, causando todo o tipo de prejuízos.

Como me proteger?
Em primeiro lugar, voltemos a enfatizar a atitude básica de evitar executar programas desconhecidos ou de origem duvidosa. Portanto, mais uma vez, *Jamais execute programas que não tenham sido obtidos de fontes absolutamente confiáveis.*

Além disto, há a questão das senhas. Se o seu micro estiver infectado outras pessoas poderiam acessar as suas senhas. E troca-las não seria uma solução definitiva, pois os invasores poderiam entrar no seu micro outra vez e rouba-la novamente. Portanto, como medida extrema de prevenção, o melhor mesmo é *NÃO DEIXAR AS SENHAS NO COMPUTADOR*. Isto quer dizer que você não deve usar, ou deve desabilitar, se já usa, os recursos do tipo "lembrar senha". Eles gravam sua senha para evitar a necessidade de digitá-la novamente. Só que, se a sua senha está gravada no seu computador, ela pode ser lida por um invasor. Atualmente, é altamente recomendável que você prefira digitar a senha a cada vez que faz uma conexão. Abra mão do conforto em favor da sua segurança.

Referências para saber mais:
Listamos abaixo alguns sites de empresas produtoras de softwares antivírus aonde você poderá atualizar periodicamente o seu programa e obter sempre as últimas novidades sobre este assunto.

- Trend Micro
- Norton Antivirus
- McAfee ViruScan
- Kaspersky AntiVírus (AVP)
- F-Secure Anti-Virus
- Computer Associates InoculateIT
- Dr Solomon's Virex Products

Command Antivirus

Procedimentos, aplicativos e dispositivos para armazenamento de dados e para realização de cópia de segurança *(backup)*.

Existem muitas maneiras de perder informações em um computador involuntariamente. Uma criança usando o teclado como se fosse um piano, uma queda de energia, um relâmpago, inundações. E algumas vezes o equipamento simplesmente falha. Em modos gerais o ***backup*** é uma tarefa essencial para todos os que usam computadores e / ou outros dispositivos, tais como máquinas digitais de fotografia, leitores de MP3, etc.

O termo ***backup*** também pode ser utilizado para hardware significando um equipamento para socorro (funciona como um pneu socorro do veículo) pode ser uma impressora, cpu ou monitor etc.. que servirá para substituir temporariamente um desses equipamentos que estejam com problemas.

Atualmente os mais conhecidos meios de ***backups*** são: **CD-ROM, DVD e Disco Rígido Externo e fitas magnéticas.** Na prática existem inúmeros softwares para criação de ***backups*** e a posterior reposição. Como por exemplo o **Norton Ghost da Symantec.**

Se você costuma fazer cópias de *backup* dos seus arquivos regularmente e os mantêm em um local separado, você pode obter uma parte ou até todas as informações de volta caso algo aconteça aos originais no computador.

A decisão sobre quais arquivos incluir no *backup* é muito pessoal. Tudo aquilo que não pode ser substituído facilmente deve estar no topo da sua lista. Antes de começar, faça uma lista de verificação de todos os arquivos a serem incluídos no *backup*. Isso o ajudará a determinar o

que precisa de *backup*, além de servir de lista de referência para recuperar um arquivo de *backup*.

Eis algumas sugestões para ajudá-lo a começar:
• Dados bancários e outras informações financeiras
• Fotografias digitais
• Software comprado e baixado através da Internet
• Projetos pessoais
• Seu catálogo de endereços de e-mail
• Seu calendário do Microsoft Outlook
• Seus favoritos do Internet Explorer

O detalhe mais importante antes de fazer um ***backup* é *formatar o disquete***. Isso pode ser feito clicando com o botão direito do mouse sobre o ícone do disquete, dentro do ícone **"Meu Computador"** e selecionar a opção **formatar.**

Para ter certeza que o disquete não está danificado, escolha a formatação completa, que verificará cada setor do disquete e mostrará para você se o disquete tem algum dano. Sempre que um disquete tiver problemas, não copie arquivos de *backups* para ele.
Bem, agora que você já sabe fazer cópias de segurança, conheça os dois erros mais banais que você pode cometer e tornar o seu *backup* inútil:

1- Fazer uma cópia do arquivo no mesmo disco. Isso não é *backup*, pois se acontecer algum problema no disco você vai perder os dois arquivos.
2- Fazer uma cópia e apagar o original. Isso também não é *backup*, por motivos óbvios.
Disquetes têm uma capacidade limitada, de 1,44 MB, e não são uma boa opção para *backups* pois logo você vai estar com uma pilha de disquetes na gaveta. Outro problema é quando você quer fazer o *backup* de um arquivo maior que a capacidade do disquete. Aí, o único jeito é recorrer a programas compactadores, como o Winzip ou o PKZip, da Pkware. Além de reduzir o tamanho do arquivo original, eles permitem fazer split, isto é, dividir o arquivo em vários pedaços de 1,4 Mb, que depois podem ser unidos novamente, com o mesmo programa.
Muitas pessoas compactam seus arquivos antes de fazer o *backup*, porque um arquivo compactado ocupa menos espaço no disquete, assim sobra mais espaço para um número maior de arquivos. Mas o correto é deixar pelo menos uma cópia descompactada dos arquivos realmente insubstituíveis. Se algo de errado acontecer com um único bit de dados de um arquivo compactado, talvez ele não possa mais ser descompactado. Procure utilizar arquivos compactados apenas como ***backups*** secundários, como imagens que geralmente ocupam um espaço muito grande.
Nesse caso, outra possibilidade é a utilização de um recurso do Pkzip que recupera arquivos danificados. Porém, nem todo o conteúdo que foi compactado será recuperado, se você copiou diversos arquivos, alguns poderão ser salvos. Se você possui um volume muito grande de arquivos para becapar, é recomendável comprar uma mídia removível, como o Zip, da Iomega. Com esses discos de 100 Mb essa tarefa vai ficar bem mais fácil. Não é o suficiente? Use discos Jaz de 2 Gb da Iomega.

Copiando Arquivos de um Disco Rígido (H.D.) para um Disquete (Fazendo Backup)

- Clique no botão “Iniciar” (canto inferior esquerdo);
- Escolha “Programas”; e no menu que abre escolha “Windows Explorer”.
- O Windows Explorer é dividido em duas partes. Do lado esquerdo são exibidas as pastas (diretórios) e do lado direito o conteúdo das pastas;
- Para ver o conteúdo de uma pasta clique uma vez sobre a pasta desejada(no lado esquerdo), e ele será exibido do lado direito.
- Para ver o conteúdo de uma subpasta (uma pasta dentro de outra pasta) clique duas vezes sobre a pasta desejada do lado direito do “Windows Explorer”;
- Depois de visualizar os arquivos ou pastas que se deseja copiar no lado direito do “Windows Explorer”, selecione-os (clicando sobre o arquivo ou pasta, este ficará destacado);
- Clique com o botão direito do mouse sobre o arquivo “Copiar”;
- Clique em Disquete de 3 ½ no lado esquerdo do “Windows Explorer”;

- Clique com o botão direito do mouse no espaço em branco do lado direito, e escolha “Colar”;

Selecionando Vários Arquivos

- Para selecionar vários arquivos ou pastas, após selecionar o primeiro segure a tecla “Ctrl” e clique nos outros arquivos ou pastas desejadas. Todos os arquivos (ou pastas) selecionadas ficarão destacadas.

Fazendo Backup do seu Outlook

Todos sabemos do risco que é não termos *backup* dos nossos dados, e dentre eles se inclui as informações que guardamos no OUTLOOK.
Já imaginou ter que entrar com todos os contatos novamente? E seus compromissos no calendário? Pior, como é que vai recuperar as mensagens de e-mail que você tinha guardado?
Como fazer o *backup* das informações do Outlook, não é uma atividade muito simples (pelo menos não há nele nada automatizado), listamos aqui algumas maneiras de executar este *backup* e se garantir contra qualquer problema! Exemplo para Outlook.

1 - Copie todas as mensagens para uma pasta separada (com isso você terá feito o ***backup*** das mensagens)
2 - Vá em Ferramentas -> Contas lá selecione todas contas que deseja salvar e selecione Exportar. Cada conta será salva com a extensão (IAF) na pasta que você quiser.
3 - Para exportar todos os seus contatos, abra o seu catálogo de endereços do seu Outlook, então clique em Arquivo -> Exportar -> Catálogo de endereços (WAB). Com esse procedimento todos os seus contatos serão armazenados num arquivo de extensão (WAB) com o nome que você quiser e na pasta que você quiser.
4 - Para as assinaturas é simples, basta copiar o conteúdo de cada assinatura que você utiliza em arquivos de texto (TXT) separados. Depois você poderá utilizar as suas assinaturas a partir dos arquivos que criou.
5 - Para as *regras* (ou filtros), você deverá ir em Ferramentas -> Assistente de Regras -> Clicar em OPÇÕES -> Clicar em Exportar Regras. Será salvo um arquivo com a extensão RWZ.

Fazer todos esses procedimentos é mais trabalhoso, porém muito mais seguro.
Outra solução, é utilizar programas específicos para ***backup*** do Outlook.

Meios disponíveis para Backups em armazenamento externo

Entende-se por armazenamento externo qualquer mecanismo que não se encontre dentro do seu PC. Existem várias opções, e apresentamos uma tabela com os mais comuns, vantagens e desvantagens:

CD-RW

É um CD em que pode guardar/gravar suas informações. Arquivos realmente preciosos que precisam ser guardados com 100% de certeza de que não sofrerão danos com o passar do tempo devem ser becapeados em CDs. A maioria dos computadores atuais inclui uma unidade para gravar em CD-RW. O CD-ROM é a forma mais segura de fazer grandes ***backups*****.** Cada CD armazena até 650 Mb e, por ser uma mídia ótica, onde os dados são gravados de maneira física, é muito mais confiável que mídias magnéticas sujeitas a interferências elétricas.

DVD-RW

É um CD mas em formato DVD.
A capacidade de armazenamento é muito maior, normalmente entre 4 e 5 gibabytes.
É necessário comprar o gravador de DVD; muitas vezes não contém software para fazer ***backups*****;** deve ser operado manualmente.

Flash USB (Pen Drive)

São dispositivos bastante pequenos que se conectam a uma porta USB do seu equipamento.

São muito portáteis, freqüentemente são do tipo “chaveiro”, ideais para ***backups*** rápidos e para mover arquivos entre máquinas.
Não têm muita capacidade; você deve escolher um modelo que não seja muito frágil.

Backups utilizando o Windows

Fazer ***backups*** de sua informação não tem que ser um trabalho complicado. Você pode simplesmente recorrer ao método Copiar e Colar, ou seja, aproveitar as ferramentas dependendo da versão do Sistema Operacional (Windows, Linux, etc) que você utiliza.

Cópias Manuais

Você pode fazer ***backups*** da sua informação com estes passos simples:

1. Clique com o botão direito sobre o arquivo ou pasta de que seja fazer *backup* e depois clique na opção “Copiar” no menu exibido.
2. Agora marque a unidade de *backup*, clique com o botão direito sobre ela e escolha “Colar” no menu exibido. Você pode marcar a unidade de *backup* ao localizá-la no ícone “Meu Computador”, ou seja, como uma das unidades do Windows Explorer.

Isso é tudo. Não se esqueça de verificar o *backup* para se certificar que ele coube na unidade de *backup* e o mantenha protegido.

Utilizando a ferramenta inclusa no Windows XP Professional.

Se você trabalha com o Windows XP Professional, você dispõe de uma ferramenta muito útil que se encarrega de fazer os ***backups*** que você marcar. Siga estes passos para utilizá-la:

1. Clique em “Iniciar” e depois em “Todos os Programas”.
2. Dentro de “Acessórios”, aponte para “Ferramentas de Sistema”.
3. Escolha a opção **“*Backup*”.**

Se for a primeira vez que você utiliza essa ferramenta, aparecerá o “Assistente de *backup* ou restauração”. Clique em Avançar e siga as instruções na tela. Se você deseja um guia passo a passo de como usar essa ferramenta, pode obtê-lo em Backup do Windows XP Facilitado (em inglês).

Sugestão: Se você não sabe qual versão de sistema operacional utiliza, dê um clique com o botão direito sobre o ícone “Meu Computador” e escolha “Propriedades”. Dentro da guia “Sistema” você encontrará a versão do seu sistema operacional.

Para utilizar a ferramenta de backups no Windows XP Home Edition.

Se seu PC tem o Windows XP Home Edition, você precisa adicionar a ferramenta de ***backups*** que vem no seu CD original seguindo estes passos:

1. Insira o CD do Windows XP (ou o que veio com seu equipamento se ele foi pré-carregado) na unidade de CD. Se a tela de apresentação não aparecer, dê um clique duplo sobre o ícone da unidade de CD dentro de “Meu Computador”.
2. Na tela de apresentação, escolha a opção “Executar tarefas adicionais”.
3. Clique em “Explorar este CD”.
4. O Windows Explorer se abrirá. Localize a pasta “ValueAdd” e dê um clique duplo sobre ela, depois em **Msft** e depois em **NtBackup**.
5. Agora, dê um clique duplo sobre o arquivo **NtBackup.msi** para instalar a ferramenta de backup.

Nota: Ao terminar a instalação, é provável que seja solicitado que você reinicie seu equipamento.
Para utilizar a ferramenta, siga estes passos:

1. Clique em “Iniciar” e depois em “Todos os Programas”.

2. Dentro de “Acessórios”, aponte para “Ferramentas de Sistema”.
3. Escolha a opção **“*backup*”.**

Se for a primeira vez que você utiliza essa ferramenta, aparecerá o “Assistente de ***backup*** ou restauração”. Clique em Avançar e siga as instruções na tela. Se você deseja um guia passo a passo de como usar essa ferramenta, pode obtê-lo em Backup do Windows XP Facilitado (em inglês).

Sugestão: Se você não sabe qual versão de sistema operacional utiliza, dê um clique com o botão direito sobre o ícone “Meu Computador” e escolha “Propriedades”. Dentro da guia “Sistema” você encontrará a versão do seu sistema operacional.

Recomendações para proteger seus backups.

Fazer ***backups*** é uma excelente prática de segurança básica. Agora lhe damos conselhos simples para que você esteja a salvo no dia em que precisar deles:

1. Tenha seus *backups* fora do PC, em outro escritório, e, se for possível, em algum recipiente à prova de incêndios, como os cofres onde você guarda seus documentos e valores importantes.
2. Faça mais de uma cópia da sua informação e as mantenha em lugares separados.
3. Estabeleça uma idade máxima para seus ***backups*****,** é melhor comprimir os arquivos que já sejam muito antigos (quase todos os programas de ***backup*** contam com essa opção), assim você não desperdiça espaço útil.
4. Proteja seus ***backups*** com uma senha, de maneira que sua informação fique criptografada o suficiente para que ninguém mais possa acessá-la. Se sua informação é importante para seus entes queridos, implemente alguma forma para que eles possam saber a senha se você não estiver presente.

EXERCÍCIOS DE FIXAÇÃO

Os gabaritos encontram-se no final dos exercícios

01) A técnica que consiste na utilização de métodos de modificação de texto, visando a não transmiti-los em sua forma clara, protegendo-os em relação a eventual interceptação, é conhecida como:
A) modulação;
B) backup incremental;
C) proxy;
D) criptografia;
E) firewall.

02) Observe as seguintes afirmativas sobre segurança em senhas de acesso.
I - Todo vírus com extensão EXE instala um programa espião para roubo de senhas.
II - Quanto menor o tamanho de uma senha, maior sua segurança.
III - Quanto maior a aleatoriedade de uma senha, maior sua segurança.
Está(ão) correta(s), somente, a(s) afirmativa(s):
(A) I
(B) II
(C) III
(D) I eIII
(E) II e III

03) NÃO é considerado um programa malicioso:
(A) *KeyLogger*
(B) *Worm*
(C) *Firewall*
(D) *Trojan*
(E) *Spyware*

04) Juvêncio recebeu um e-mail reportando que seu CPF estava cadastrado no Sistema de Proteção ao Crédito. Mesmo não havendo possibilidade disso acontecer, pois paga suas contas em dia ele, inadvertidamente, clicou no link que havia no corpo do e-mail. O link remetia para o seguinte endereço: http://www.vocecaiu.com/invadi.exe. A partir desse momento, o programa executado (invadi.exe) se instalou na máquina e capturou sua senha de banco. Esse é um procedimento característico de infecção por:
A) vírus de boot
B) vírus de macro
C) worm
D) trojan
E) spam

05) Considere as assertivas abaixo sobre criptografia:
I. Criptografia é o conjunto de técnicas matemáticas utilizadas para embaralhar uma mensagem.
II. Na criptografia simétrica a mesma chave é utilizada para encriptar e decriptar uma mensagem.
III. Na criptografia assimétrica são usadas duas chaves, uma privativa e uma pública.
Estão corretas:
A) I e II apenas
B) I e III apenas
C) II e III apenas
D) I, II e III
E) Todas estão incorretas

06) Não são propriedades da comunicação segura:
(A) confidencialidade e disponibilidade;
(B) autenticação e criptografia;
(C) disponibilidade e controle de acesso;
(D) integridade e não-repúdio de mensagens;
(E) roteamento e escalonamento.

07) .Em relação aos vírus de Informática, NÃO é um objetivo desses programas:
A) retardar o processamento da máquina;
B) introduzir figuras ou objetos em movimento na tela, atrapalhando a visualização dos dados e dificultando seu processamento;
C) apagar todas as informações contidas no disco rígido do equipamento;
D) causar destruição dos programas e aplicativos;
E) prover alimentação elétrica sem interrupção para os servidores e equipamentos ativos, evitando uma interrupção brusca no processamento.

08) Em relação às formas de contaminação por vírus na Informática, aquela que é considerada a maior forma de contaminação por vírus é:
A) disquete de driver do fabricante de placa de vídeo;
B) arquivos da Internet;
C) CD-ROM (R) oficial de instalação do Windows;
D) jogos com licenças e mídias oficiais;
E) arquivos do backup.

09) Sobre segurança na Internet, considere as afirmativas a seguir.
I. Sempre abrir arquivos anexados a e-mails.
II. Manter sempre um programa anti-vírus instalado e atualizado.
III. Instalar um firewall para aumentar a segurança.

IV. Clicar em links de bancos recebidos por e-mail.
Apresentam hábitos que diminuem os riscos no uso da Internet, apenas as afirmativas:
a) I e II.
b) II e III.
c) I e IV.
d) I, III e IV.
e) II, III e IV.

10) Para impedir que usuários não autorizados abram um documento, você deve:
a) atribuir uma senha em Ferramentas - Opções - Salvar
b) No menu Ferramentas, clique em Proteger documento.
c) Salvar como e marcar a caixa de seleção Recomendável somente leitura.
d) Salvar como página da web

11) O dispositivo físico, utilizado para realizar uma cópia de segurança local, que permite o resgate de informações importantes ou programas em caso de falha do disco rígido, pode ser definido como:
A) Backup;
B) Restore;
C) Sistema Operacional;
D) Disquete;
E) Browser.

12) Dentre as alternativas a seguir indique qual é a CORRETA quando se quer definir, no ambiente Internet, o que significa spam:
A) mensagens eletrônicas enviadas para usuários sem que estes as tenham solicitado.
B) conjunto de endereços de domínios inexistentes.
C) bloqueadores de endereços de domínios inexistentes.
D) nome de um vírus que se espalha via correio eletrônico.

13) Selecione a melhor forma de privacidade para dados que estejam trafegando em uma rede:
A) Criptografia.
B) Chaves de segurança e bloqueio de teclados.
C) Emprego de sistema de senhas e autenticação de acesso.
D) Métodos de Backup e recuperação eficientes.
E) Desativação da rede e utilização dos dados apenas em "papel impresso".

14) Sobre as cópias de segurança também chamadas de "backup", podemos afirmar:
A) Backup´s de arquivos e de banco de dados são procedimentos extremamente necessários nas instalações de informática das organizações. Eles não permitem re-processamentos, mas, entre outras finalidades, permitem recuperar transações processadas.

B) Backup´s de arquivos e de banco de dados são procedimentos extremamente necessários nas instalações de informática nas organizações. Eles não permitem re-processamentos, mas, entre outras finalidades, permitem recuperar situações passadas e facilitam trabalhos de auditoria.

C) Os backup´s e log´s (histórico) de transações são fundamentais em atividades de auditoria e na recuperação de transações processadas, possibilitando re-processamentos.

D) É uma boa estratégia fazer um backup total do sistema diariamente, principalmente em ambientes com grandes bases de dados.

E) Os backup´s geralmente são gravados em dispositivos com grande capacidade de armazenamento e de alta velocidade de acesso para facilidade das operações.

15) Sobre o hardware utilizado para armazenamento de dados e informações nos computadores, podemos afirmar:

A) Os discos magnéticos são unidades exclusivamente de saída e servem para armazenar os arquivos e banco de dados das aplicações nos computadores.

B) Todo disco magnético e CD-ROM, nos ambientes de microcomputadores, podem ser re-utilizados (regravados).

C) Os arquivos de dados e de aplicações são gravados nos discos magnéticos e no CD-ROM numa estrutura constituída por trilhas concêntricas.

D) Os arquivos de dados e de aplicações são gravados nos discos magnéticos numa estrutura constituída por trilhas concêntricas, todas com a mesma capacidade de armazenamento.

E) Nas trilhas mais próximas do centro (raio menor) dos discos magnéticos e dos CD-ROM, a quantidade de informações gravadas é menor do que nas suas trilhas mais externas (raio maior).

16) Um funcionário utiliza o webmail corporativo da empresa em que trabalha. Ele recebe uma mensagem com o assunto "urgente", contendo um arquivo anexo executável, mas não reconhece o nome do remetente.
Entre as atitudes a seguir, qual representa maior risco para a segurança do sistema?
A) Abrir o arquivo imediatamente. Pode ser importante.
B) Deixar a mensagem guardada, mas sem abrir, aguardando algum contato telefônico que indique sua origem.
C) Apagar a mensagem imediatamente. Se ele não conhece o remetente, não está esperando nenhuma mensagem dele.
D) Abrir e ler a mensagem, mas não executar o anexo.
E) Tentar descobrir quem é o remetente, ligando, por exemplo, para a telefonista da empresa.

Gabarito

01 - D	02 - C	03 -C	04 - D	05 - D	06 - E	07 - E	08 - B	09 - B	10 - A
11 -D	12 - A	13 - A	14 - C	15 - D	16 - A	***	***	***	***