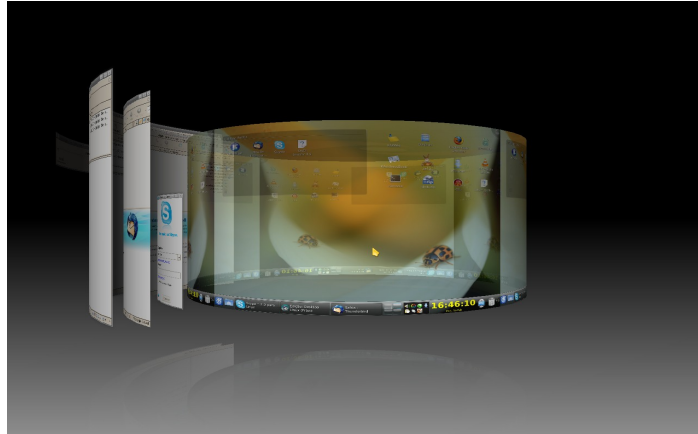


# A segurança da informação em um computador II

Computadores não são máquinas seguras, ninguém que tenha um pingão de juízo e que conheça o mais básico de um computador deixaria alguma informação nele depositada que pudesse ser classificada como de segurança ou vital para as suas necessidades, mesmo que fosse este computador o seu, pessoal, e destinado exclusivamente para o seu uso.



Sistema de telas do Linux Kubuntu

Escrevi isto no mês passado, também escrevi que: O computador na realidade é uma ameaça maior aos usuários em geral sob aspectos outros muito mais importantes até mesmo que a segurança das informações que o incauto usuário guarda ciosamente em seu interior certo que estão estas absolutamente seguras, ou ainda nos nos trabalhos e documentos que mais ingênuos ainda enchem de senhas e depois os colocam na rede mundial, felizes da vida, para apreciação pública.



São três os pontos fracos na segurança dos computadores:

O primeiro está nos próprios componentes físicos de um computador, e em especial no seu processador.

O segundo está nos programas que são utilizados pelos mesmos para as suas inúmeras tarefas.

O terceiro está na conexão destes computadores com outras máquinas e o resto do mundo.

No primeiro caso a falha esta na fabricação dos componentes, o usuário nunca sabe com certeza o que estes componentes estão fazendo além daquilo para que foram construídos, é muito fácil para os fabricantes inserir nestes componentes rotinas, normalmente binárias, para a execução de ordens que nada tem a haver com a sua função original, tais funções podem ser ativadas com comandos de origem remota se conectados com o resto do mundo, por tempo de operação do sistema ou ainda por comandos inseridos no computador pelo próprio usuário; o potencial destrutivo ou não para este tipo de falha é simplesmente astronômico e se eu, um miserável usuário, consegui ver isso imagina só o que não estão vendo os entendidos no assunto.



O segundo caso a falha tem como princípio básico o mesmo princípio do primeiro caso, o ingênuo usuário jamais ficará sabendo o que mais o programa que ele acabou de instalar ira fazer além do que ele se propôs a fazer, se você acha que o seu sistema de programas faz apenas o que diz que veio para fazer você é um tolo, um programa de computador pode fazer milhares de operações e apenas a que você que que seja feita ele estará sempre (quando não trava) lhe mostrando, você sempre verá e obterá aquilo que espera ver e obter e nunca verá ou obterá nada além disso; tenha em mente o seguinte: um programa de computador faz aquilo que o seu programador mandou fazer mas lhe mostrará sempre aquilo que você espera ver e nunca o que realmente está a fazer; o potencial de destruição desta falha é gigantesco mas não chega nem aos pés do potencial que representa o primeiro caso.



O terceiro caso é o de menor poder destrutivo, pois é apenas o meio de entrada dos comandos acionadores para o primeiro e segundo caso e é também o caminho de saída para o furto de informações; é também a porta de entrada para programas não nativos ao sistema, programas estes que levará o seu computador para o segundo caso de falha na segurança através de programas normalmente pequenos cujas intenções via de regra são inconfessáveis.

Como anular todas estas ameaças?

Isso não é possível, se esta opção de ação partir do usuário.

A única maneira de se eventualmente evitar um mal maior é fechando todas as portas de entrada e saída de seu computador, mesmo assim com a alta tecnologia das máquinas de hoje receio não ser isso suficiente, posto que as mesmas possuem meios de comunicação sem o uso de cabos e por aí basta apenas que as mesmas estejam conectadas a uma fonte de energia e tudo voltará à mais completa das inseguranças.

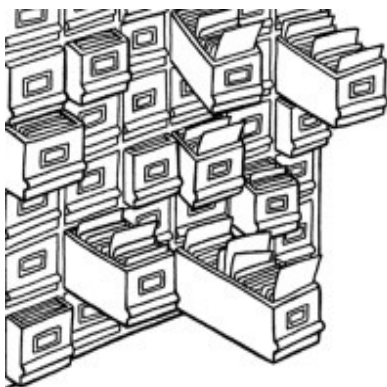
No entanto é possível dificultar as coisas mas evitar uma eventual catástrofe não.



A primeira forma é não usando o computador para guardar nada que lhe seja vital e fazendo com que o processo de passagem destas “vitalidades” pelo seu computador seja o mais breve possível; tudo o que lhe for vital deve ser guardado fora do computador e de outros eletrônicos sempre.

Segundo, se a primeira forma não for possível então guarde estas informações em HD diferente daquele usado pelo sistema operacional e pelos programas, use um HD exclusivo para a guarda de dados de preferência em meio a outros HDs mais além do que já foi citado para o uso do sistema operacional e seus programas.

Terceiro, se nada do que anteriormente escrito for possível, minha sugestão é que desmembre a informação, criptografe as partes desmembradas com criptogramas diferentes e as espalhe pelo HD, se mesmo esta opção não for possível e como agravante você ainda tem que estar conectado com o mundo exterior a minha sugestão é só uma: Reze, e o faça com muita, muita fé mesmo (quem sabe né?).



Quarto, nunca, eu vou repetir; **NUNCA** guarde o que lhe é vital em um lugar, seja ele qual for, fora da sua máquina, fora do alcance de sua visão, fora de seu controle pessoal; fazer isso é passar e assinar um atestado de estupidez tão grande, que faria a ideia de “astronomicamente grande”, ficar reduzida ao tamanho de um elétron apenas.

Quinto, tenha em mente sempre o seguinte: Computador seguro é todo aquele que não esta conectado, fisicamente ou não, com outras máquinas; que esteja desligado de toda e qualquer fonte de energia e que por fim, esteja completamente desmontado e que suas partes, uma vez separadas, sejam guardadas em um local inserto ou ignorado, até mesmo por você.



São Paulo, 30 e junho de 2011

mkmouse