Segurança do Sistema Operacional Microsoft

Por Paulo Bindo

Após o surgimento da Internet ouço que os produtos Microsoft são vulneráveis, qualquer um pode invadi-los e todos os vírus os atacam. Lembro-me que em Janeiro de 2002 a Microsoft anunciou uma campanha mundial chamada de "Trustworthy Computing", com o objetivo de treinar todos seus profissionais em relação à importância da segurança nos sistemas e revisar todos os códigos de programas para sanar possíveis falhas de segurança.

Muitos devem pensar que os programas Microsoft eram os únicos a ter problemas de segurança, mas se analisarmos os históricos de outros softwares veremos que muitos hackers ou crackers (hackers ruins) estão familiarizados com uma variedade de antigas brechas de segurança do UNIX. É por isso que a Apple gastou muito tempo e esforço certificando-se para que o OS X fosse seguro a partir de seu lançamento.

Sabemos que um Software livre nasceu do Unix e se pesquisarmos na Internet verá que alguns problemas de segurança não foram corrigidos até hoje. O risco de uma empresa ter suas informações nas mãos de pessoas mal intencionadas é alto e pode custar muito caro.

Em relação aos vírus vamos voltar a uns anos atrás e relembrar do Code Red e Nimda que atacaram milhares de servidores através de falhas do sistema operacional; Porém estas falhas já haviam sido divulgadas e corrigidas pela Microsoft e caso os servidores estivessem atualizados, os vírus não conseguiriam agir. Vejamos também do vírus que atacou o SQL sendo que já havia uma correção evitar o ataque; Isto demonstra que segurança não depende somente do fabricante, mas principalmente dos profissionais de TI.

Foi pensando em segurança que existe uma campanha da Microsoft voltada à segurança chamada Academia Latino Americana de Segurança da Informação [http://www.technetbrasil.com.br/academia/] e esta é voltada para qualquer tipo de sistema operacional, já que aborda conceitos de segurança.

A Microsoft preocupa-se tanto com a segurança de seus produtos que passou a fornecê-los com seus serviços desabilitados, assim o Administrador da rede tem de habilitá-los e configurá-los conforme suas necessidades; Para os usuários inexperientes existirá um ambiente totalmente seguro.

Não existe um sistema operacional 100% seguro e livre de falhas, então vamos fazer uma análise nos casos em que o sistema precise de uma correção:

- A Microsoft possui uma equipe própria que corrige e testa, para uma rápida solução e utiliza-se do WUS - Windows Update Service para disponibilizá-los aos usuários dando a liberdade dos mesmos instalar ou não conforme sua necessidade, de forma simples e confiável.

- Quanto a um software livre fica difícil sabermos se uma falha foi totalmente corrigida e testada. Quem garantirá que não foi inserido um código malicioso nesta suposta correção? Em quanto tempo esta falha será corrigida? Em qual local encontrar a correção? E se existir mais que uma correção disponível em qual confiar? Quem aplicará esta correção?

Existe um site [https://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/alertus.asp] da Microsoft para o profissional de TI encaminhar uma possível descoberta de vulnerabilidades para que uma equipe interna avalie e dê andamento a possíveis correções caso sejam necessárias.

Conclusão

A Microsoft está fornecendo seus softwares com a máxima segurança possível e está treinando seus clientes através da Internet para que os mesmos possam introduzir mais segurança em suas redes.

Como podemos ver existem muitas vantagens para um Administrador de rede ou um usuário final em trabalhar com softwares que possuem uma equipe altamente qualificada, treinada e que irá apresentar uma única solução segura em um curto espaço de tempo em relação aos demais softwares de mercado.

Paulo Bindo

Inicio da pagina