01 – Abril de 1999

Proteção corporativa, agora de dentro para fora.

As formas de se fazer negócio estão mudando e as preocupações também. Com a crescente competitividade, impulsionadas pela abertura dos mercados e a globalização, as empresas se viram obrigadas a agarrar a tecnologia para agregar valor aos seus negócios e reduzir os custos. Passaram, então, a disponibilizar informações importantes na rede corporativa, nos computadores portáteis dos executivos e nas mensagens de correio eletrônico que são enviadas diariamente. Confiaram ao meio magnético a segurança do seu negócio.
Não demorou muito, e logo perceberam o potencial da Internet como meio de comunicação pela abrangência, padronização e custo. Pois bem, cheguei onde queria: a segurança.

Neste exato momento, milhares de computadores estão conectados a uma enorme malha de comunicação, espalhados por todo o planeta e trocando informações incessantemente. Muitas delas sem valor. Mas uma boa quantidade, potencialmente poderosa, circulando livremente.
Com a expansão da Internet, da Intranet e do acesso remoto - revelando-se verdadeiras portas de entrada e saída para o mundo - os sistemas passaram a ficar vulneráveis aos ataques externos. Pensando nisso, o *firewall*, tradicional na interligação entre LANs e WANs e na proteção de acesso aos servidores com a separação da rede interna da externa, vem cumprindo – quando bem configurado - seu papel inicial. Mas se o acesso externo está em parte equacionado por esta solução, não se pode dizer o mesmo dos acessos à dados externos pelos usuários da rede interna.

O modelo atual para segurança das redes tem assumido que o "inimigo" está do lado de fora da empresa, enquanto que dentro, todos são confiáveis. Esta idéia tem feito com que a grande maioria dos administradores de rede utilizem uma estratégia de segurança que restringe o acesso para qualquer usuário externo e, por outro lado, libera de forma irrestrita o acesso aos servidores para a totalidade dos usuários internos. Esta estratégia, embora simples, não é adequada já que estatísticas recentes apontam as ameaças internas como as responsáveis por grande parte das sabotagens, fraudes, invasões, ataques por vírus e acessos indevidos.
Então, se o acesso externo já não é a principal vulnerabilidade, como solucionar os problemas de acesso interno ?

A resposta está próxima. Em virtude do grande alcance global das redes, do crescente poder de ação das informações contidas nos computadores, da possível perda de produtividade e do potencial de destruição e invasão dos atuais “vírus” como os Trojan Horses (Cavalo de Tróia) percebeu-se uma exigência maior de níveis de segurança e controle de acessos diferentes, o que mostrou a tendência do *firewall* em se tornar uma solução mais fragmentada para proteger cada área da empresa de forma específica e até mesmo cada estação da rede. Surge então o *firewall* pessoal.

O ***firewall* pessoal** veio na verdade, trazer um conceito complementar ao *firewall* tradicional. Quando utilizado nas estações de uma rede corporativa, dá-se à elas o controle

e a privacidade sobre as informações armazenadas e aos administradores da rede, o controle dos acessos realizados por elas à informações externas. Portanto, com uma só ferramenta, garantimos a privacidade dos dados da corporação e controlamos os acessos externos, evitando a perda de produtividade por mau uso.

Nesse momento, muitos de vocês devem estar imaginando que esta solução está distante da realidade de suas empresas e associando-a à um objeto de filme do agente 007, mas contrariando as expectativas, ela está se tornando uma opção cada vez mais popular.
Cada vez mais fornecedores estão anunciando a utilização de recursos de VPNs (Virtual Private Networks) ponto à ponto, que incorporam a criptografia entre as extremidades de uma conexão e permitem que as organizações criem "túneis" seguros ao longo da Internet, implementando assim o conceito de *firewall* "pessoal".

Portanto, se você e sua empresa já se sentem completamente seguros depois da instalação de um firewall tradicional, levante-se da cadeira e comece a pensar em proteger as informações que sustentam seus negócios e estão circulando na rede corporativa, absorvendo o conceito do irmão mais novo do *firewall*: o *firewall* pessoal.

Marcos Sêmola *é MBA em Tecnologia Aplicada e Consultor de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br