

FACULDADE GAMA FILHO
SEGURANÇA DE REDES
PROF. RICARDO BARROSO

Parte II - Identificando os principais problemas de segurança

Existem diferenças fundamentais na segurança voltada para o mercado corporativo onde nos deparamos com a utilização de tecnologias avançadas com alta capacidade de tráfego e gerenciamento de estações quando comparadas à segurança voltada para o mercado doméstico, do usuário da internet ou da dona de casa que guarda suas receitas no micro (microcomputador, não microondas, ainda...). ;-)

O objetivo do nosso curso básico é ajudar a resolver os problemas do usuário doméstico, aquele que lê seus emails, faz sua pesquisa escolar ou consultas para seu escritório e aquele que usa computadores por diversão em bate-papos, jogos, paqueras etc. Neste capítulo estaremos mostrando os principais atentados à segurança que você pode sofrer usando o seu computador pessoal.

Estes atentados se dividem em três grandes categorias que muitas vezes estão interligadas, sendo necessário um ataque à uma categoria antes de se iniciar ataques as outras. São elas: (1) ataques à privacidade, (2) destruição e (3) obtenção de vantagens.

Ataques à privacidade - Este é o ataque direto mais comum ao usuário doméstico. Assim como muitas pessoas têm compulsão em ler correspondência alheia ou observar vizinhos com lunetas, hackers têm compulsão em "dar uma olhadinha" na sua vida pessoal e a melhor maneira de se descobrir coisas sobre a vida de uma pessoa é olhando dentro do seu computador. Os principais alvos são os seus emails mandados, recebidos e apagados, seu histórico de visitação de sites ou seus "arquivos.doc", onde podem conter cartas, procurações, contratos e até aqueles poeminhos que você fez e jurou jamais mostrá-los a alguém.

Destruição - Apesar de ser perfeitamente possível para um hacker, uma vez estando dentro do seu computador, destruir seus dados, as estatísticas mostram que na grande maioria dos incidentes nos quais há perdas de informação a causa é a ação de vírus ou programas com funções semelhantes, que raramente são implantados de forma proposital. Geralmente a infecção ocorre com programas recebidos de terceiros que muitas vezes também não sabem que estão infectados. As conseqüências podem ser as piores, pois os usuários domésticos não têm o costume de fazer backups dos dados do seu computador pessoal.

Obtenção de Vantagens - Para se obter vantagens causando incidentes de segurança nos computadores pessoais geralmente é necessária a utilização de técnicas onde primeiro a vítima será exposta a ataques de privacidade ou destruição. As motivações deste tipo de ataque são tão distintas quanto seu próprio objetivo real.

Por exemplo, garotos podem invadir computadores de amigos para obter informações ou destruir dados com o único intuito de se vangloriar perante a vítima derrotada, atitude normal nas definições de status e liderança em qualquer grupo animal. Outros podem ter objetivos mórbidos, como o simples prazer na destruição, sem importar-se com a sua tese de mestrado na qual trabalhou quase dois anos. E, como não poderia deixar de ser, as vantagens financeiras estão presentes com uma fatia assustadora dos objetivos de ataques a computadores pessoais.

Faça isso agora: classifique a informação presente no seu computador pessoal. Não só a informação que fica armazenada nele mas, principalmente, a informação que "**passa**" por ele. Você verá que a informação armazenada, apesar de ter toda a sua atenção e preocupação, corresponde a apenas parte do problema no caso de uma quebra de segurança no seu computador. Você pode não deixar gravado no seu computador o número do seu cartão de

crédito ou a sua senha do internet banking, mas esta informação, após ter sido digitada, faz parte do seu computador temporariamente. O que alguns hackers fazem é monitorar seu computador e esperar por informações deste tipo. Com esta informação na mão eles podem abandonar seu computador e quem sabe até fechar a porta por onde eles entraram para não levantar futuras suspeitas. O último a sair apaga as luzes!

Com base apenas nestas informações, tente responder às seguintes perguntas: Você usaria hoje, em seu computador pessoal, um programa de internet banking para fazer transferências de dinheiro? Você faria compras na internet, mesmo sabendo que o site/loja possui um servidor seguro, digitando seu cartão de crédito no seu computador pessoal? Você trataria de assuntos importantes na sua vida pessoal e profissional, na qual se utiliza de dados particulares, através de simples emails? Caso tenha respondido "não" às três perguntas, responda mais essa: Para que serve a internet?

Felizmente temos meios de impedir - ou, pelo menos, de dificultar enormemente - as ações que põe em risco nossa vida online. O risco sempre vai existir, assim como existe na nossa vida fora dos bits e bytes. A questão é trazer o "grau de risco" a um nível aceitável, de modo que possamos evoluir na utilização da tecnologia até um patamar mais confiável e conseqüentemente mais eficaz, porque, sem segurança, a internet não vai passar de uma grande idéia ou de um caro brinquedo.

Enjoy ☺