



**Marcos Flávio Araújo Assunção**

*Considerado um dos especialistas mais importantes em Hackerismo Ético do mundo, consultor de nível internacional em Segurança de TI. Citado em fontes como o New York Times, como um dos principais piratas cibernéticos, foi responsável pela dissolução de redes criminosas e terroristas internacionais no cyberspaço. Especialista Certificado pela ECCouncil - Certificadora mundial para Hackers Éticos (USA - Novo Mexico). Formado em Engenharia de Software pela UNA / Belo Horizonte. Marcos também é conhecido pelo desenvolvimento de softwares para uso corporativo contra invasões. Publicou diversos livros no assunto.*

## **Ingenuidade Empresarial**

Cada dia mais as empresas sofrem com o vazamento de informações altamente secretas, como dados confidenciais de seus produtos ou e-mails de sua base de clientes. A velocidade com que essas ações vêm ocorrendo é assustadora, mas, o que mais assusta é a ingenuidade da maioria dos empresários em relação à esse problema.

Hoje, vivemos uma guerra constante no mundo da informação. Ações que despencam de um dia para o outro, empresas declarando falência ou tentativas de fusão que buscam a sobrevivência de uma grande marca. Com o mundo em crise, os que obtêm sucesso não são mais aqueles que possuem o maior capital e sim os que dominam o controle da informação.

A informação é mais importante do que qualquer produto existente na face da terra. O que acontece na maior parte dos casos é que, infelizmente, ela não recebe um nível satisfatório de proteção. Muitas empresas parecem viver em uma espécie de mundo de "faz de conta", no qual elas não investem na segurança da sua informação como deveriam e acreditam que nada de mal irá acontecer. Essa ingenuidade é um problema muito mais sério do que parece, pois essa falsa sensação de segurança é justamente o que os hackers e os engenheiros sociais apreciam.

Um bom exemplo está no próprio investimento em segurança. Para certas organizações, basta instalar um anti-vírus que sua rede está protegida. Algumas outras entendem a necessidade de um bom firewall. E ainda há aquelas que chegam até a implementar um sistema de detecção de intrusos. Todas essas soluções de proteção citadas podem até impedir determinados ataques mais simples mas não funcionam contra um invasor mais experiente.

Por exemplo: através de dois processos chamados de footprinting e firewalking, um hacker pode identificar as regras de proteção de seu alvo, o sistema operacional das máquinas da rede, e possivelmente até mesmo as contas de usuários. Com essas informações em mãos ele sabe que técnica pode utilizar para burlar os filtros e conseguir

chegar ao seu objetivo. Normalmente tais técnicas utilizam recursos de tunelamento para dificultar a detecção do ataque.

Para a questão tecnológica então, uma solução simples seria partir do conceito das listas brancas. Bloqueia-se todo o acesso interno e externo e aos poucos libera-se o que pode ser acessado. Dessa forma é bem mais simples ter um controle melhor sobre o que é permitido, diminuindo o risco de um "grampo eletrônico" permitir acesso à um invasor externo.

Agora, isto ainda nem começa a corrigir o problema. Preocupar-se com a tecnologia é importante mas de nada adianta se ignorarmos o fator humano. As pessoas são muito mais fáceis de serem manipuladas do que a tecnologia. Para que se dar ao trabalho de descobrir uma senha de acesso se simplesmente podemos nos passar por alguém da TI e pedir a um funcionário desavisado? Isto é Engenharia Social, o que podemos definir de modo bem resumido como "a Arte de enganar".

A Engenharia Social é a forma mais utilizada hoje para realizar espionagem empresarial. Seja por telefone, internet ou pessoalmente, o Engenheiro Social tem muitas maneiras distintas para poder atuar. A situação se torna particularmente grave se somarmos essas maneiras ao fato de muitas empresas não realizarem um filtro adequado de spam, um bom controle de acesso físico ou uma política adequada de classificação de informações. Um exemplo de vulnerabilidade: alguém com acesso físico ao ambiente pode instalar um capturador de teclas em uma máquina e enviar tudo o que for digitado para outro local.

Qual a solução para o fator humano? Treinamento constante e conscientização. A organização de workshops e realização de campanhas que mostrem como combater a Engenharia Social minimizam o efeito destes ataques em qualquer companhia. Mas isso não deve ser feito apenas uma vez, mas em intervalos regulares, demonstrando novos golpes e como evitá-los.

Após citar todos os problemas uma coisa deve ficar bem clara. Não podemos mais nos dar ao luxo de sermos ingênuos. Se um único problema, humano ou tecnológico, uma única vez, permitir acesso de um espião à base de dados da empresa, acabou-se. Anos de trabalho perdidos em meros segundos.

Lembre-se: segurança não é reparar, é prevenir. Prevenção é sempre a chave.