64 - Fevereiro de 2005

A culpa é nossa.
Comportamento faz toda a diferença.

O que está por trás das novas ameaças que colocam em risco a confidencialidade, integridade e disponibilidade das informações? Qual é o real gerador dos impactos provocados por uma rede de computadores inoperante, pelo vazamento de informações confidenciais, pela interrupção de processos de negócio e a paralisação de uma linha de produção?
Instintivamente somos levados a responder as perguntas baseando-nos na primeira percepção das ameaças que estão mais próximas dos fatos mencionados. É verdade que um vírus de computador pode ter tornado toda sua a equipe improdutiva temporariamente por impedimento de acesso a um sistema ou ainda, que a falta de energia possa ter interrompido seu fluxo de produção. Mas são percepções distorcidas que só dificultam a análise da situação e minimizam o poder de prevenção e reação.
É notório que o conhecimento do ser humano cresce ano a ano e assim, o fruto da aplicação desse mesmo conhecimento. Novas tecnologias, novas ferramentas, novas formas de se fazer a mesma coisa. É o progresso e suas inovações. Os vírus de computador, as técnicas de ataque, os sistemas eletrônicos de controle de transmissão de energia ou ainda as máquinas que suportam um processo produtivo mudaram e continuarão mudando,
portanto, o que parece ser a causa dos riscos de hoje, só fazem esconder seus verdadeiros responsáveis: as pessoas.

Independente do lado em que estejam seja na proteção ou no ataque, as pessoas são os reais agentes de ameaça e que diariamente exercitam formas diferentes de alcançar seus objetivos. Há décadas, quando o termo “vírus de computador” se popularizou através de pequenos programas escritos em linguagens nada amigáveis de programação e se limitavam a hospedar-se na trilha zero de velhos discos de 360 kbytes para embaralhar a tela de fósforo verde do monitor, quem estava por trás eram os mesmos agentes que agora estão por trás dos “modernos”, ao menos até o próximo semestre, vírus polimórficos. A arma mudou, acompanhou a evolução tecnológica, mas sua eficácia continua e continuará atrelada à deficiência das extremidades, ou seja, do comportamento dos usuários e técnicos.

Se na época aquele vírus era considerado uma ameaça real, era porque conseguia explorar falhas comportamentais dos usuários, que por sua vez, potencializava a exploração de outras falhas técnicas intermediárias. Sabemos que os sistemas e maquinas falham, mas estar atendo a eles e soluciona-los no menor tempo possível e papel das pessoas.
Não culpem os antivírus, pois são igualmente intermediários no processo de geração de risco. Muitos são realmente eficazes, mas tornam-se incapazes de cumprir integralmente o seu papel porque foram mal “instruídos” por seus controladores. Se um vírus ou spyware copiou e corrompeu sua base de dados foi provavelmente porque alguma pessoa não atualizou a vacina ou simplesmente porque foi irresponsável ao executar um programa de fonte desconhecida. Se o sistema de fornecimento de energia falhou e seu ambiente era crítico e pouco tolerante à falhas, houve incompetência de alguém no provisionamento de

uma solução alternativa compatível com a sensibilidade do ambiente. Se informações armazenadas em meios físicos ou mesmo digitais, vazaram, não foi porque a rede estava frágil ou porque o processo de criação e manutenção de senhas era falho, mas porque os agentes que estavam por trás deles não souberam projetar situações de risco e adotar os controles adequados, seja na especificação da arquitetura da rede seja na elaboração de uma política de senhas rígida o bastante.

O comportamento das pessoas diante de medidas e contramedidas de segurança faz toda a diferença. A perenidade dos seres humanos é certa e, apesar da tendência apontar para um cenário de cada vez menos interação, eles sempre estarão por trás das decisões, dos controles e das armas. Essas sim, tendem a mudar muito rapidamente. Desta forma, não seria nada inteligente montar uma estratégia de segurança baseada na variável da equação, na porção mais imprevisível, quando a peça chave e felizmente, aquela que já se conhece há tempos, continua sendo o homem.

Marcos Sêmola *é South America Security Consulting Manager da multinacional Atos Origin, Consultor Sênior em Gestão de Segurança da Informação, profissional certificado CISM – Certified Information Security Manager pelo ISACA, BS7799 Leader Auditor pelo BSI, Membro do Computer Security Institute, Professor de Segurança da Informação da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus e eleito pelo prêmio SecMaster, Profissional de Segurança da Informação de 2003 cat4.*
marcos@semola.com.br