77 – Julho 2006

Em segurança da informação, menos pode ser mais.

Simplificar tem sido meu desafio nos últimos 7 anos escrevendo e falando sobre gestão dos riscos da informação em aulas e palestras. Acredito que empresas e *Chief Information Security Officers*, em geral, deveriam canalizar seus esforços focando no tratamento das ameaças e riscos mais relevantes, e assim, investir tempo e dinheiro na parcela mais significativa dos problemas. Esta abordagem não revela nenhuma novidade, mas por vezes não os vemos com comportamentos práticos coerentes com este pensamento e antes mesmo que antigos e conhecidos problemas sejam solucionados ou tratados definitivamente, já os pegamos pensando e procurando resolver novos problemas.

Mais uma vez o conceito de Paretto parece aplicável e vem nos dizer que, também em segurança, 80% dos problemas podem ser gerenciados com apenas 20% de esforço. Posso estar redondamente enganado e meu exercício de simplificação pode ir por água abaixo em um futuro breve, mas para mim neste caso, Menos pode significar Mais.

O que estou tentando dizer não ignora a evolução e o dinamismo das ameaças, falhas e incidentes, mas se baseia fundamentalmente na percepção de que muitos dos problemas de segurança são conceitualmente comuns a todo negócio e continuam presentes, apesar de serem muitas vezes, tratados como problemas ultrapassados que já não merecem ou retém a atenção dos profissionais de segurança da informação. Momentaneamente, o segmento de segurança parece seguir o movimento do mercado de alta tecnologia ou o mercado de moda, onde técnicas e produtos tornam-se velhos e desatualizados pela simples existência de uma novidade. O resultado disso é a desorientação e o entusiasmo descabido por projetos novos, sem antes mesmo estar certo de que os antigos foram bem sucedidos.

Faca um exercício e resgate da memória a lista de problemas e incidentes de segurança que foram identificados em sua empresa nos últimos meses. Agora imagine como esta lista seria diferente se alguns dos antigos problemas relacionados à senha, permissão de acesso, atualização de sistemas, vírus, controle de conteúdo, classificação de documentos, backup, segregação de rede e mídia removível tivessem sido resolvidos, ou ao menos, tivessem sido prioritariamente administrados. Pois é justamente a isso a que me refiro.

Não posso negar a importância da segurança sob medida, nem tão pouco de todos os potenciais controles e processos necessários para sustentar a operação de um completo sistema de gestão de riscos da informação, promovendo o aumento dos níveis de controle e maturidade. Entretanto, não me parece coerente se preocupar com os problemas mais modernos enquanto os mais antigos e conhecidos permanecem desassistidos. Não vejo como uma sábia decisão, por exemplo, existindo limitações financeiras e temporais, gastar o exíguo orçamento com um ambicioso projeto de gerenciamento de identidades enquanto os perfis de acesso continuam sem segregação e as senhas sem uma política forte.

Na prática, me pergunto, por exemplo, por que um longo projeto de análise de riscos para identificar e classificar a potencialmente extensa lista de vulnerabilidades se previamente muitas delas já são conhecidas e são suficientemente complexas para consumir todo o tempo de sua equipe e seu orçamento? Por que mobilizar os *stakeholders* e representantes das áreas chaves da empresa para escrever uma política de segurança se sabidamente existem diretrizes e normas prontas que podem ser incorporadas imediatamente mediante uma ou outra adaptação, sem muito esforço e com alta efetividade? Foi pensando assim que surgiu esta breve lista de ações:

- Defina regras e uma estrutura para gerenciamento de senhas de acesso. Procure soluções que permitam o cancelamento e a renovação da senha pelo próprio usuário. Aliado a isso, aprimore o modelo de segregação de funções, definição de perfis, acesso remoto, monitoramento e auditoria de permissão de acesso, inclusive sobre os recursos do sistema operacional. Estes fatores juntos são responsáveis por grande parte dos problemas relacionados ao acesso indevido e à perda de informação por falha humana.
- Classifique as informações e defina regras de conduta para o manuseio, armazenamento, transporte e descarte nos formatos físico e digital. Sem estes parâmetros e o conhecimento deles, quem poderia ser um aliado da segurança não poderá ajudar e quem poderia oferecer risco sequer tomará conhecimento do fato de estar descumprindo a política.
- Segregue física e logicamente sua rede de dados com base na classificação da informação e nos requerimentos de acesso as aplicações e serviços. Projete cenários possíveis de acesso não autorizado, de indisponibilidade e especialmente de contaminação por vírus. Este esforço será recompensado por uma rede mais inteligente tanto no monitoramente pró-ativo de ameaças quanto na administração reativa de incidentes. Como em um edifício, se a estrutura de tubulação de distribuição de água e a segregação através de registros for inteligente, não será um simples vazamento em um dos cômodos de um andar específico que interromperá o abastecimento de todos os moradores.
- Invista em soluções de backup inteligentes e compatíveis com a sensibilidade das informações e do negócio. Defina claramente os processos de backup, documente-os, teste-os frequentemente e treine os operadores, pois tanto as falhas humanas quanto as ameaças intencionais e naturais são responsáveis por parcela significativa das interrupções e impactos no negocio.
- Estabeleça procedimentos e uma rotina de gerenciamento de atualizações de segurança utilizando sua atual estrutura de gerenciamento. A lacuna de tempo entre a descoberta de uma nova vulnerabilidade e a aplicação de uma correção determinará seu nível de exposição ao risco. Mesmo assim, não planeje logo uma estrutura de reação D+0 ou D+1 no primeiro instante, pois esta decisão pode requerer altos investimentos, enquanto que a simples decisão de criar de um processo de *patch management* já o colocará em outro patamar de segurança.
- Concentre boa parta da sua energia na estratégia de controle de conteúdo malicioso, vírus e no controle de mídias removíveis. Implemente uma solução corporativa de

antivírus independente da ação do usuário, garantindo atualização e varreduras orientadas ao ambiente. Filtros de acesso à Internet e controle de dispositivos removíveis de armazenamento poderão reduzir consideravelmente os problemas com vazamento de informação.

Simplificando:

1. Defina critérios de criação e renovação de senhas de acesso
2. Segregue perfis e permissões de acesso aos sistemas
3. Segregue física e logicamente a rede de dados
4. Limite o acesso aos recursos do sistema operacional
5. Limite o uso de dispositivos removíveis
6. Implemente uma solução de antivírus e controle de conteúdo
7. Implemente solução de gerenciamento de atualizações de segurança
8. Classifique as informações e defina os procedimentos de manipulação
9. Documente e teste periodicamente as rotinas de backup
10. Adote políticas de segurança para os temas acima e treine os usuários

Ainda como alça de realimentação, assuma a necessidade de acompanhar os resultados das 10 ações para avaliar o retorno, extrair lições aprendidas e promover melhorias continuas. Estou certo de que terá sido um bom e consistente começo.

E lembre-se: o que não se conhece não se pode controlar. O que não se controla não se pode mensurar. O que não se mensura não se pode gerenciar e o que não se gerencia não se pode aprimorar.

Marcos Sêmola *é Consulting Business Development da multinacional Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, profissional certificado CISM – Certified Information Security Manager pelo ISACA, BS7799 Lead Auditor pelo BSI, Membro da ISACA, ISSA, IBGC, CSI e membro fundador do IISP – Institute of Information Security Professionals of London. Professor da FGV – Fundação Getúlio Vargas, Pós Graduando em Negociação e Estratégia pela London School, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed. Campus, autor de outras duas obras ligadas à gestão da informação pelas editoras Saraiva e Pearsons e premiado pela ISSA como SecMaster®, Profissional de Segurança da Informação de 2003/2004, sendo membro da comissão julgadora em 2005. Visite www.semola.com.br ou contate marcos@semola.com.br*