26 – Novembro de 2000

7+7 Dicas para proteger o seu negócio - parte 2

Dando continuidade ao artigo anterior, seguem as outras 7 dicas para elevar o nível de segurança do seu negócios, reduzindo ao máximo os riscos:

8. Policy Enforcement
Aplicação da Política de Segurança em português faz parte da Implementação de Segurança. Softwares que seguem critérios pré definidos de utilização dos recursos tecnológicos, seja nos servidores ou estações de trabalho, e até mesmo uma equipe de auditoria, podem ser os responsáveis pelo sucesso da adesão das pessoas às diretrizes, normas, procedimentos e instruções que regem a política de segurança. Não esqueça de agir com transparência se for aplicar tais recursos, afinal, você quer seus funcionários como aliados.

9. Termo de Sigilo
Questionado por muitos e aplicado por alguns, o termo de sigilo representa um pacto de compromisso entre a empresa e o funcionário no que tange o uso correto dos recursos tecnológicos a ele disponibilizados. Não existe um respaldo legal, mas já é uma iniciativa de comprometê-lo com o sucesso da empresa na integração entre tecnologia e negócio. Seu sucesso está diretamente ligado à conscientização comentada na dica número 1.

10. Teste de Invasão
Tem seu importante papel pondo à prova - com a segurança assegurada por um especialista - o ambiente corporativo ao utilizar as técnicas e ferramentas mais difundidas nos meios underground. Software de sniffer (grampo digital), Denial of Service (negação de serviço), Trojan Horses (cavalos de tróia), Trashing (análise de lixo) e engenharia social são terminologias dessa etapa.

11. Plano de Contingência
Garantir a continuidade de processos ou informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos do desastre. Com este propósito e formado pelas etapas: estratégias de contingência, planos de retorno e os procedimentos de contingência propriamente ditos, o plano de contingência deve ser escrito para ser verdadeiramente executado, portanto, deve ser realista. Janela de tempo, tolerância à paralisação, gatilhos de acionamento e rotas alternativas de comunicação são alguns dos parâmetros analisados.

12. Administração de Segurança
A busca pela segurança deve ser uma atividade constante, afinal, quando uma nova tecnologia se incorpora ao ambiente corporativo, novas vulnerabilidades à acompanham. Desta forma, as macro etapas: análise, política e implementação, devem ser refeitas visando a atualização. Segurança é um processo cíclico.

13. Security Office
Expressão nova para muitos, mas já uma realidade para as empresas modernas, o Security Office é um cargo, uma ocupação cada vez mais importante. A segurança eletrônica é percebida como fator crítico de sucesso e por isso precisa ser planejada e coordenada por quem realmente a tem como competência básica. Alguém que pense em segurança o tempo todo e que acompanhe a evolução tecnológica, reduzindo o tempo de defasagem entre a descoberta de uma nova vulnerabilidade e sua solução.

14. Solução Corporativa de Segurança da Informação
Pense no negócio e não apenas em soluções pontuais. Trace uma estratégia focada na busca do Enterprise Security Planning!

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor da cadeira de Segurança da Informação da FGV – Fundação Getúlio Vargas, Gerente de Produto e Analista de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br