25 – Novembro de 2000

7+7 Dicas para proteger o seu negócio - parte 1

Há muito venho esboçando a vontade de escrever um artigo mais objetivo e prático. Algo como uma lista de atividades fundamentais para garantir a segurança corporativa. Um conjunto de dicas e procedimentos. Assim, motivado ainda mais pelos últimos e-mails que tocaram justamente no assunto, aqui está!

1.Conscientização
É fator crítico de sucesso conseguir o comprometimento dos altos executivos e não menos importante preparar as pessoas para a mudança de cultura. Seminários de conscientização, onde explica-se a importância da segurança e o papel das pessoas no cenário corporativo são fundamentais.

2. Análise do Negócio
É preciso analisar o paciente antes mesmo de receitar qualquer medicamento. O mesmo se pode dizer da empresa. A solução de segurança tem de visar o negócio e não somente ambientes, processos e tecnologias isoladas. Mesmo que não se possa implementar simultaneamente em toda empresa, é necessário que os projetos se encaixem e estejam bem definidos em um amplo plano diretor de segurança. A análise do negócio deve acontecer através de entrevistas, onde se pode levantar a competência básica, a cultura da empresa, o fluxo de informações, os processos críticos e consequentemente os ativos (infra-estrutura, aplicações, processos e pessoas) merecedores de uma análise mais profunda.

3. Análise das Vulnerabilidades
Dando continuidade, essa etapa permitirá identificar as vulnerabilidades e priorizá-las de acordo com sua criticidade. A análise do ambiente predial permitirá o conhecimento dos aspectos físicos da segurança no que diz respeito a incêndio, instalações elétricas, cabeamentos lógicos, condições climáticas e controle de acesso físico seguindo o conceito de perímetros de segurança. A análise de documentos é importante para que políticas corporativas, especificações técnicas, regras de configuração de ambiente e até mesmo normas de qualidade sejam levadas em consideração. A análise do ambiente informatizado é a etapa complementar. Servidores, Estações de Trabalho, Firewalls, Roteadores, Switches, Links e equipamentos de conectividade em geral são analisados tecnicamente a procura de vulnerabilidades que potencializem as ameaças.

4. Política de Segurança
Esquecida por muitas empresas, a política de segurança talvez seja um dos fatores mais importantes para garantir a segurança corporativa. Isso porque ela trata justamente do ativo - ou elo, se fizermos analogia à uma corrente - mais esquecido: as pessoas. É o conjunto formado por diretrizes, normas, procedimentos e instruções que irá nortear os usuários quando ao uso adequado dos recursos à eles disponibilizados. Onde se definem regras, comportamentos, proibições e até punições por má utilização. Este documento igualado - com as devidas proporções - à importância da constituição de um país, tem de ser escrito

sob medida. Deve estar de acordo com a cultura da empresa e seus recursos tecnológicos, para então, ser seguido e não apenas representar um grande volume de papel empoeirado e esquecido. Regras de manutenção e criação de senhas, rotinas de backup, fragmentação de material descartado, limites para uso de e-mail e a definição de trilhas de auditoria são alguns dos pontos abordados.

5. Classificação da Informação

Complementando a política de segurança, a classificação da informação é responsável por descrever os procedimentos para seleção, manipulação, transporte, armazenamento e descarte de informações, identificando-as de acordo com a sua importância. Com base no perfil do negócio e característica das informações que circulam no ambiente corporativo, estabelece-se um padrão de classificação como por exemplo: Confidencial, Restrito, Interno e Para Divulgação. Desta forma, todos saberão como se comportar diante das informações que manipulam.

6. Campanhas de Divulgação

Com as pessoas conscientizadas pelos seminários e a política de segurança elaborada, surge um novo desafio: fazê-las seguir o que foi definido. Pensando justamente em tornar essa tarefa mais fácil, as campanhas de divulgação segmentam todo o enorme conteúdo da política de segurança, focando nas normas, procedimentos e instruções ligadas ao dia-a-dia de cada departamento da empresa. As pessoas passam então a receber informação filtrada, o que certamente trará mais eficiência. Cartazes nos corredores e e-mails informativos completam a iniciativa.

7. Implementação de Segurança

Chegou a hora da verdade. Depois de conhecer as vulnerabilidades, agora priorizadas por criticidade (impacto x risco), cruzadas com as necessidades inerentes à cada ambiente e a atividade do negócio, aplica-se soluções de hardware e software - um vasto leque de ferramentas que se integram - que garantirão o nível de segurança especificado no plano diretor de segurança. Antivírus, hot-fixes e patches de correção de sistemas operacionais, certificados digitais, salas-cofre, criptografia, smartcard, software de Intrusion Detection, Virtual Private Network, roteador, firewall e aplicações Public Key Infrastruture, são algumas das soluções pontuais que podem compor o ambiente.

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