

Quem Torna as Empresas Vulneráveis?

Adriana Gobbo (ILLIX Tecnologia e Inteligência)
Marco Antonio dos Santos (Prospect Intelligence)

O acesso à informação tornou-se uma necessidade estratégica para as organizações neste início de terceiro milênio, por questões ligadas à lucratividade, competitividade, segurança ou, até mesmo, à sobrevivência. Estruturalmente, tornamo-nos produtores e consumidores vorazes de informações.

Dessa maneira, é imprescindível proteger esse ativo, muitas vezes intangível, do alcance de pessoas ou entidades sem escrúpulos, que possam fazer mau uso dele, atingindo mortalmente a organização.

Recentemente, ao fazer uma consultoria para uma grande empresa, cujo capital principal é seu banco de dados, encontramos um quadro grave e, preocupantemente, muito comum em empreendimentos nacionais: infelizmente, não temos cultura de sigilo e de preservação de assuntos críticos.

A empresa teve todos os seus arquivos de clientes roubados por "hackers" a serviço de um concorrente, que passou a usufruir o valor deles. Os danos e percas foram de monta para a vítima.

A primeira medida adotada pela direção da empresa foi buscar proteção em aparatos tecnológicos, uma vez que não dispunha de quase nada nesse sentido, mediante consultores especializados em TI. Ação apropriada, porém insuficiente. A insipiência da decisão, uma vez que a empresa continuou sendo lesada, deveu-se à não implementação de um plano integrado de Segurança da Informação, que contemplasse todas as vertentes de acesso ao núcleo do capital informacional da entidade: Tecnologia da Informação (TI), verificação das instalações, documentos desprotegidos e sem classificação e pouco conhecimento sobre pessoal interno.

Verificamos que a estrutura física não era adequadamente segura, que documentos e materiais permaneciam facilmente acessíveis e a política de pessoal era totalmente inadequada ao tipo, ao ambiente de negócios e à conjuntura deste terceiro milênio.

A análise diagnóstica permitiu verificar que a extração das informações, embora tivesse acontecido por meio eletrônico, havia sido facultada por elemento humano, fonte primária de dados por excelência.

Confirmando aquilo que Kevin Mitnick explora em seu livro "A Arte de Enganar", a empresa havia sido objeto de um ataque de "Engenharia Social" arquitetado por operadores habilidosos. Não são objetos de apreciação neste artigo os aspectos ético e criminal da ação (em si condenável).

Normalmente, os engenheiros sociais exploram as motivações humanas, fazendo uso de métodos e técnicas especializadas de extração de dados, quase sempre à revelia da fonte, ou mediante o aproveitamento de alguma fraqueza própria dos seres sociais.

A maioria das evasões de informações acontece com o ataque ao elo mais fraco da cadeia organizacional. Cerca de 70% das ocorrências, para ser um pouco mais exato, ocorre com o concurso de funcionários, alvos de operações bem planejadas e como principal entrada para qualquer sistema tecnológico.

O elevado turn over, a facilidade de obter no mercado pessoas com elevada capacitação (principalmente pela taxa de desocupação presente), os downsize e reengenharias mal estruturadas, as terceirizações e quarteirizações que carrearam as empresas para um sentimento de insegurança e de "necessidade de ganhos rápidos", terminaram por fazer com que funcionários não mais vestissem a camisa da organização. A consequência mais imediata foi a vulnerabilidade.

Sofisticação tecnológica e seus custos elevados em casos como acima mencionados não podem ser vistas como medidas isoladas. A tecnologia deverá ser uma ferramenta nas mãos de pessoas treinadas e reeducadas para a cultura do sigilo empresarial.

Muitas implementações de Segurança de TI são consideradas ineficientes - e isto é justificável - que adianta um avançado sistema de monitoramento eletrônico, se as pessoas envolvidas não participam do ciclo de segurança corporativo? Ou ainda, se os altos escalões mantêm-se fora do monitoramento ou não seguem as políticas de segurança da informação?

Sendo assim, a elaboração séria de estratégias de segurança

compreendendo plano de negócio, orçamentos, análise de concorrentes, análise de pontos fortes e fracos, entre outros, torna-se fator crítico para sobrevivência das companhias. Mas, além disso, e prioritariamente, os dirigentes devem promover uma nova cultura: O mundo tornou-se perigoso demais para a ingenuidade empresarial.