

É notório que no mundo de TI temos notícias de vazamento de informações, ou mesmo o uso das mesmas para obter vantagens ilícitas. Casos como os notebooks furtados de um container da Petrobras podem refrescar nossa memória sobre casos famosos que recentemente apareceram na mídia. E, então, fica a pergunta: como proteger tanta informação?

A teoria de proteção de perímetro é a primeira que vem a nossa mente. Firewall, IDS, IPS, entre outros, aparecem como soluções para barrar hackers dos nossos Datacenters. “Manteremos os invasores do outro lado do muro!” gritaria um Gerente de TI mais exaltado. Mas, muitas vezes o inimigo está ao lado!

Uma pesquisa feita pelo Ponemon Research Institute, divulgada em março deste ano, entrevistou mil pessoas que perderam o emprego nos últimos 12 meses. Desse total, 59% admitiram ter roubado informações confidenciais da empresa, 79% levaram informações sem autorização e 82% declararam que seus ex-empregadores não realizaram nenhum tipo de auditoria em seus documentos, notebooks, etc, antes de serem demitidos.

Quanto maior é o conhecimento de como funciona uma organização, maior é, também, a facilidade de fraudar, roubar ou mesmo alterar informações que levem a algum tipo de prejuízo financeiro ou mesmo de imagem da empresa perante ao mercado.

Qual é a confiança de um consumidor sobre uma empresa que não protege seus dados? E seus fornecedores? Qual o tamanho do prejuízo de uma imagem de “empresa sem segurança” perante o mercado? É difícil mensurar os prejuízos, mas é fácil saber que não serão pequenos se eles acontecerem.

A implementação de políticas de segurança da informação passa, necessariamente, por soluções de DLP – Data Loss Prevention, ou “Prevenção Contra Perda de Dados”.

Classificar as informações é o primeiro passo e o mais importante deles. É preciso localizar, analisar, quantificar o nível de sensibilidade da informação (seu nível de confiabilidade). O próximo passo é definir regras de acordo com as políticas de segurança da informação da empresa, tais como:

- Se o arquivo tiver um determinado nível de segurança, quais usuários poderão copiar via USB/CD para fora do desktop/notebook?
- Um usuário pode copiar para seu desktop/notebook uma informação que está no servidor de arquivos da empresa?
- Que tipo de informações podem ser enviadas por e-mail, ou mesmo em arquivos anexo?

Após estes passos concluídos, o último estágio é monitorar a adequação dos usuários às políticas implementadas – fase permanente mesmo após a conclusão de um projeto de DLP, pois os processos de uma empresa mudam de acordo com suas necessidades de crescimento, estratégia e governança. E as políticas de segurança mudam junto com os processos.

As chaves do sucesso de um projeto DLP são:

- Apoio da alta cúpula da empresa - como em qualquer projeto de segurança da informação;
- Iniciar por nichos – primeiro alguns departamentos e expandi-los ao longo do tempo para toda empresa;
- Análise correta das informações e seu nível de sensibilidade;
- Flexibilidade da solução de DLP.

O último item trata da “des-burocratização” da segurança da informação no dia-a-dia de uma empresa. Exemplo: se um estagiário não pode enviar e-mail com uma planilha de orçamento,

um diretor talvez possa. Mas se ele puder, é obrigatório que ele registre de forma transparente e rápida o motivo de enviar tal arquivo.

Isto evita a propagação de comentários como “o pessoal de segurança só serve para atrapalhar minhas atividades” ou “o departamento de Segurança da Informação só piora a minha produtividade” e tantos outros comentários (injustos) que os profissionais de segurança estão acostumados a ouvir.

Artigo escrito por Vitor Augusto Villafranca, gerente de Prática de Segurança da Kaizen.