>> White paper
Março | 2010

Experimente contratar um provedor de SGS para aumentar a eficácia do seu orçamento

arcon
serviços gerenciados de segurança
15 anos

Ambiente de segurança da informação

O ambiente de segurança da informação é realmente desafiador: ameaças cada vez mais potentes, velozes e sofisticadas, padrão de ataques migrando da tentativa de causar indisponibilidade para as tentativas de roubo ou uso de informação sensível com o objetivo de ganhar dinheiro, abertura das redes corporativas ao acesso remoto, uso intensivo de dispositivos de computação móvel, descentralização dos acessos à Internet, pressão interna para liberação do uso de redes sociais na rede corporativa, virtualização, adoção de sistemas "*on the cloud*" e, finalmente, o aumento inexorável da pressão regulatória sobre a gestão da informação.

Para lidar com os desafios impostos o profissional de segurança da informação precisa utilizar um arsenal de ferramentas (leia-se sistemas de segurança) complexas e difíceis de operar. Porém, ao comprar e implantar uma ferramenta dessas, a única coisa garantida é a despesa com a sua aquisição e implantação, invariavelmente alta. Isto porque a relação entre a qualidade da ferramenta escolhida e o resultado obtido é fortemente influenciada pela qualidade da implementação e da operação diária. Adquirir uma boa ferramenta realmente não garante o resultado esperado. Assim sendo, é razoável avaliar a possibilidade de contratar serviços especializados para selecionar, implantar e operar as ferramentas necessárias como forma de maximizar o resultado da aplicação do orçamento para proteção da informação.

Quais os motivos para terceirizar segurança da informação?

Por que as corporações procuram empresas especializadas para ajudá-las a gerir suas operações de segurança? Custo é um bom motivo, mas não é o único, e nem deveria ser o primeiro. A lista abaixo, que não tem a pretensão de esgotar o assunto, fala dos mais frequentes:

- Obter, manter e reter os profissionais com o conhecimento adequado para proteger a informação no complexo e mutante ambiente de TI, além de caro pode ser simplesmente inviável para a maioria das corporações. Isto porque os profissionais de segurança são naturalmente atraídos pelas empresas especializadas em busca de uma carreira no setor.

- O tempo para implementar novas soluções de segurança é sempre curto. Mesmo que a empresa possua profissionais capacitados na tecnologia, dificilmente os terá em quantidade e com disponibilidade suficientes para fazê-lo no tempo esperado. Empresas especializadas possuem estes recursos disponíveis como parte do modelo de negócio.

- Os profissionais das empresas especializadas, em contato permanente com múltiplas ameaças simultâneas em diversos ambientes, estarão mais preparados para combater ameaças que os profissionais dedicados a um único ambiente corporativo, por maior que ele seja.

- Para muitas corporações este é um bom atalho para obter a padronização dos procedimentos de segurança e atender a requisitos regulatórios.

- É um meio de obter garantias contratuais de que os requisitos de segurança serão cumpridos. A despesa deixa de ser a única coisa garantida. Em um contrato bem feito, se os objetivos de negócio não são atingidos, a despesa não acontece.

© Arcon Serviços Gerenciados de Segurança. Todos os direitos reservados.

E por que o custo pode ser menor na terceirização?

Empresas especializadas em operar sistemas de segurança da informação compartilham recursos de toda ordem entre os diversos clientes e, por isso, conseguem oferecer profissionais, infra-estrutura e sistemas de segurança em regime 24 x 365 a uma fração do que seria possível fazer internamente ***atingindo o mesmo nível de requisitos.***

Para citar apenas um exemplo, imagine que uma organização precisa avaliar, adquirir, implantar e operar um novo Sistema de Gerenciamento de Eventos de Segurança (SIEM - Security Information and Event Management). Se limitarmos a escolha apenas aos líderes do segmento teremos ao menos 9 soluções de diferentes fabricantes. Imagine quanto custa o processo para entender, testar e homologar uma solução entre as nove pré-selecionadas. Isso feito é necessário comprar, treinar pessoal, desenhar processos, implantar e operar a nova solução. Certamente essas atividades serão executadas com pessoal a ser contratado, dado que a equipe atual já deve estar no limite da sua capacidade. Caso o resultado não seja satisfatório não há o que fazer a não ser começar tudo de novo desperdiçando tempo e o dinheiro investido.

Agora, se pensarmos que uma empresa especializada na oferta deste sistema, possivelmente com dezenas de clientes dispostos a utilizá-lo, rateará uma boa parte destes custos por todos os contratantes e que os clientes só pagarão se o resultado for o estabelecido em contrato, podemos ter uma ideia do potencial de economia e de redução de riscos intrínsecos ao processo de terceirização. Mas por que potencial? Bem, as coisas também podem dar errado se o processo de seleção e contratação de um terceiro não for feito no momento e da forma corretos.

Quem são as empresas especializadas nestes serviços?

Os provedores de serviços gerenciados de segurança (Managed Security Services Providers - MSSP) são empresas que implantam e operam soluções de segurança fornecidas como serviço, usualmente monitoradas, gerenciadas e administradas remotamente através de Centros de Operação de Segurança (Security Operations Centers - SOCs). Os MSSPs se encarregam da seleção, aquisição, implantação e operação de soluções de segurança que são pagas mensalmente pelas empresas contratantes com base em metas e resultados, na forma de prestação de serviços. As soluções de segurança fornecidas vão desde a proteção da borda da rede com Firewall/VPN, IPS e Gateways de proteção de e-mail e acesso a web, passam pelo controle do acesso à rede e proteção local de estações de trabalho e servidores e terminam em sofisticados sistemas de prevenção contra o vazamento ou perda de informações (DLP) e a correlação e gerenciamento de eventos de segurança (SIEM).

Riscos na adoção

Não é razoável esperar que todos os problemas sejam resolvidos logo após a assinatura do contrato de terceirização. Alguns riscos devem ser avaliados e gerenciados antes, durante e depois do processo. Capacidade do provedor para lidar com aspectos específicos da organização, confiança na capacidade da contratada, manutenção do sigilo das informações gerenciadas pelo serviço, manutenção das equipes internas responsáveis pelo contrato e pelo seu resultado, delineamento de uma estratégia para reverter a dependência do provedor caso ele saia do mercado ou não performe adequadamente, são algumas

© Arcon Serviços Gerenciados de Segurança. Todos os direitos reservados.

questões a serem observadas para reduzir os riscos de fracasso do processo de terceirização. Para facilitar as coisas é fundamental que a organização inicie esse processo com objetivos de segurança bem definidos e com um rigoroso critério de avaliação das empresas candidatas.

Como avaliar os fornecedores?

Sem o risco de cometer erros podemos agrupar os MSSPs em quatro grandes categorias: unidades de segurança de empresas de telecomunicações, unidades de grandes integradores de TI, boutiques especializadas em operacionalização de sistemas de segurança da informação e unidades de prestação de serviços de fabricantes de produtos de segurança da informação. Algumas empresas prestam serviços dessa natureza sem necessariamente se encaixar em nenhum desses grupos, normalmente adotando uma estratégia oportunista para aumentar a receita em uma carteira estabelecida de clientes, porém não há nenhum benefício claro em contratá-las para tal.

A seleção entre empresas de cada grupo traz benefícios específicos para cada tipo de contratante. Empresas de telecomunicações normalmente fornecem serviços de gerenciamento da borda da rede – Firewall/VPN e IPS – como complemento dos serviços de telecomunicações. Contratantes com redes muito dispersas e baixos requisitos ténicos e funcionais de segurança podem se beneficiar dessa abordagem, especialmente no que se refere ao custo. As grandes integradoras de TI são especialistas no relacionamento profundo com o cliente e caso este esteja plenamente satisfeito com os serviços, não demande soluções muito criativas e se sinta seguro em ampliar o escopo do contrato, deve avaliar essa possibilidade com o seu fornecedor atual de TI. Adotar um fabricante como prestador de serviços pode ser interessante se já existir um forte relacionamento com o fornecedor através de seus produtos e se estes atenderem plenamente as necessidades de quem avalia. As empresas especializadas em segurança são as mais adequadas quando os requisitos principais são a qualidade técnica, a capacidade de inovar e desenhar soluções sob medida e a visão holística e de longo prazo da segurança.

Alguns requisitos, seja qual for o grupo a que pertence o fornecedor a ser avaliado, não podem ser considerados como trunfos, mas antes, condições mandatórias para participar do jogo. Não é razoável avaliar fornecedores que não tenham, no mínimo, o seguinte:

- Infra-estrutura de alta disponibilidade e tolerante a falhas com, ao menos, dois SOC operando 24 x 365. Cada um desses centros de operação deve ser capaz de lidar isoladamente com todos os clientes do fornecedor.

- Equipes amplamente capacitadas em segurança e com profissionais certificados pelos fabricantes dos produtos utilizados para prestar os serviços em todos os turnos. Experiência da equipe e baixa rotatividade também são igualmente relevantes.

- Processos e sistemas de gestão que atendam as melhores práticas de gestão de TI em geral e da segurança da informação em particular.

- Capacidade de entregar relatórios frequentes, consistentes e úteis sobre todos os aspectos dos serviços contratados.

- Portal do cliente para abertura e acompanhamento em tempo real do tratamento de solicitações e incidentes.

- Portifólio de soluções capaz de atender a todas as demandas atuais e futuras do cliente, evitando assim múltiplos relacionamentos com fornecedores do mesmo tipo.

© Arcon Serviços Gerenciados de Segurança. Todos os direitos reservados.

- Capacidade financeira para acompanhar as demandas da empresa contratante e garantir a continuidade dos negócios durante a expectativa de duração dos contratos.

O que é importante no processo de contratação?

A preparação para o processo de terceirização é fundamental para reduzir o risco de insucesso. As corporações precisam, em primeiro lugar, ter objetivos de segurança claramente definidos e orçamento para atingí-los. Deve ser possível exprimir esses objetivos em termos quantitativos e estes devem ser colocados em acordos de nível de serviço (Service Level Agreements - SLAs) que impliquem em multas significativas para o fornecedor quando não atingidos. De acordo com esses mesmos objetivos, devem ser estabelecidos critérios claros de seleção dos fornecedores de modo a não utilizar apenas o preço e características técnicas de produtos para escolher a melhor proposta.

Uma vez escolhido o fornecedor as atenções devem se concentrar no processo de implantação de soluções e transferência de responsabilidades. Exigir e validar um processo detalhado de transferência pode economizar muito dinheiro e resguardar as reputações dos patrocinadores dos projetos. Por último, mas não menos importante: planeje a saída do contrato com cuidado. Problemas acontecem e a melhor maneira de minimizá-los é assumir que eles podem ocorrer e planejar a solução com antecedência.

© Arcon Serviços Gerenciados de Segurança. Todos os direitos reservados.

Sobre a ARCON

Atuando no mercado nacional há quinze anos, a Arcon é uma empresa especializada em serviços gerenciados de segurança (MSS Managed Security Services). A companhia tem por missão selecionar, implantar, monitorar e operar, com eficiência e proatividade, sistemas de proteção da informação que maximizem o resultado dos investimentos e aumentem o nível de segurança das empresas de médio e grande porte do Brasil.

Seu portifólio abrange os serviços de Firewall, IPS, Gateway Web, Gateway SMTP, Proteção de Endpoint, Proteção contra Vazamento de Informações (DLP) e Correlação de Logs e Eventos (SIEM) que utilizam tecnologia de empresas como Trend Micro, Websense, SourceFire, RSA, Checkpoint, Cisco, Blue Coat e Microsoft.

Com SOCs redundantes localizados nas cidades do Rio de Janeiro e São Paulo e uma equipe de profissionais de segurança certificados e altamente capacitados, a Arcon gerencia mais de 290 ativos de segurança em todo o País, os quais protegem mais de 125.000 estações de trabalho e servidores de clientes de diversas verticais, entre elas finanças, telecomunicações, governo, indústria, saúde, energia e educação.

Nos últimos quatro anos a empresa cresceu a uma média de 70,1% ao ano, conquistou mais de uma centena de clientes e firmou-se como referência no mercado brasileiro de MSS, tendo conquistado ainda o segundo lugar no ranking INFO Exame das empresas de TI que mais cresceram em 2008.

Rio de Janeiro
Av. Pres. Vargas, 3.131 sala 1603
20.210-911 Cidade Nova
Tel: 21 3293.1000

São Paulo
Av. Ibirapuera, 2.332 cj 52
04.028-002 Moema
Tel: 11 3525.1800

www.arcon.com.br

©Arcon Serviços Gerenciados de Segurança. Todos os direitos reservados.