Folha Info

COMPRAS ONLINE DE NATAL CRESCEM

Estudo do serviço de pesquisa de preços BuscaPé indica que as vendas pré-Natal desse ano superaram as do ano passado em 36%. Os resultados foram obtidos tomando por base o faturamento de 1.780 empresas que vendem algo pela internet, entre os dias 5 e 11 de dezembro. O segmento que mais cresceu nos últimos 12 meses foi o de eletrônicos, com 41% a mais de vendas agora. Em segundo lugar, vêm produtos de informática e brinquedos (ambos com crescimento de 31%).

| ENTREVISTA: MARCOS SÊMOLA |

Sua informação está segura?

FELIPE ANDRADE E ALEX OLIVEIRA
(cpd@fmanha.com.br)

A partir de agora, toda última terça-feira do mês, vamos trazer para os leitores da **Folha da Manhã** entrevistas com especialistas ligados à área de Tecnolgia de Informação. Não poderíamos começar melhor. Estamos entrevistando o profissional Marcos Sêmola, que é um dos mais conceituados especialista em segurança da informação no Brasil e no mundo. Direto de Londres, onde vive atualmente, Marcos Sêmola é Consulting Business Development da Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, profissional certificado CISM — Certified Information Security Manager pelo ISACA, BS7799 Lead Auditor pelo BSI, Membro da ISACA, ISSA, IBGC e do Computer Security Institute, Professor da FGV — Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação — uma visão executiva, Ed.Campus, autor de outras duas obras ligadas à gestão da informação pelas editoras Saraiva e Pearsons e premiado pela ISSA como SecMaster®, Profissional de Segurança da Informação de 2003/2004. Caso queria mais informações, visite o site de Marcos em www.semola.com.br ou contate marcos@semola.com.br.

ARQUIVO PESSOAL

Folha da Manhã – O que vem a ser segurança da informação?
Marcos Sêmola – O problema pode se tornar complexo, mas o conceito e tão simples quanto proteger conhecimento sob forma de informação, garantindo sua confidencialidade, integridade e disponibilidade.
Confidencialidade – Propriedade de manter a informação a salvo de acesso e divulgação não-autorizados.
Integridade – Propriedade de manter a informação acurada, completa e atualizada.
Disponibilidade – Propriedade de manter a informação disponível para os usuários, quando estes dela necessitarem.
Sob o ponto de vista da solução, Segurança da Informação é: "adotar controles físicos, tecnológicos e humanos personalizados, que suportem a redução e administração dos riscos, levando a empresa a atingir o nível de segurança adequado ao seu negócio."

Folha – Como é possível criar uma política de segurança?
Marcos – Definir política de segurança não e tarefa fácil, especialmente por que a expressão pode assumir um significado diferente dependendo da abrangência. Entretanto, podemos simplificar as coisas definindo-a como um conjunto de ações que consideram ativos físicos, tecnológicos e humanos para estabelecer políticas (diretrizes, normas e procedimentos) e processos de gestão de riscos que suportem um programa de governança de riscos da informação.

"A segurança se faz em pedaços, porém todos eles integrados, como os elos de uma corrente"

O principal desafio da empresa é ter uma visão integrada dos riscos. A segurança se faz em pedaços, porém todos eles integrados, como os elos de uma corrente. Se você fortalece um elo (os sistemas) e deixa outro (as pessoas, ou "peopleware") de lado, a corrente não fica segura. Por isso, o primeiro desafio é conseguir enxergar a segurança em todos os aspectos — físicos, tecnológicos e humanos — e tratar todos eles de forma igualitária. As questões de segurança não podem mais ser atribuídas simplesmente à ação de hackers. Dependem também do comportamento dos funcionários, de documentos formais que estabeleçam uma política de segurança e criem uma cultura nas pessoas, e da segurança física nas próprias instalações.
E lembre-se: política de segurança tem que ser personalizada e portanto, escrita de acordo com a natureza do negócio, sua tolerância ao risco, perfil dos ativos e requerimentos de segurança.

Folha – Como as empresas podem e devem agir na segurança de seus dados?
Marcos – A base de uma política de proteção esta na classificação da informação.
A política de classificação da informação deve estabelecer procedimentos para seleção, manipulação, transporte, armazenamento e descarte seguro de informações de forma a orientar usuários e ativos, de um modo geral, a como se comportar diante de uma informação classificada, por exemplo, como sensível, interna ou publica. Elas precisam de um tratamento diferente em cada fase de seu ciclo de vida e todos os ativos que custodiam a informação, sejam eles físicos, tecnológicos ou humanos, precisam estar em conformidade com essa política.
Com a classificação definida e disseminada, se pode ampliar a aplicação dessas regras aos demais ativos como equipamentos de rede, sistemas/permissões de acesso, processos de armazenamento, backup etc..

Folha – Hoje, estamos ouvindo falar muito em fraude na internet. O que é? e como pode ser combatida?
Marcos – A Internet e apenas um dos ambientes suscetíveis a invasão ou quebra de confidencialidade, integridade e disponibilidade. Assim como a rede interna, gateways de acesso remoto ou outros meios de comunicação e armazenamento de dados, a Internet oferece riscos. Por sua forte presença no ambiente corporativo e sua característica de rede mundial pública, ela tende a ser o ponto mais vulnerável e por isso merecedor de maior atenção.
Contudo, pesquisas confirmam anualmente que a maior ameaça a segurança da informação não vem da Internet, mas dos funcionários da própria empresa, seja por erro ou ação intencional.

Folha – Muitos spam atrapalham o andamento de empresas hoje. Como podemos evitar essa praga?
Marcos – Se usar a Internet é navegar, estamos literalmente boiando no meio de muito lixo. Não estamos navegando, pois com tanto obstáculo e sujeira, fica impossível assumir uma velocidade de cruzeiro. De acordo com o Gartner, o velho conhecido SPAM já é responsável por mais de 34% dos emails que circulam pela grande rede no ano de 2005. Evitar o SPAM não e tarefa fácil, especialmente por que não há uma identidade estática que facilite a identificação de um SPAM. Entretanto, muitas ferramentas baseadas em conhecimento mantido por especialistas 24 horas por dia, 7 dias por semana, 365 dias ao ano, prometem identificar com velocidade novas formas de SPAM, atualizar a lista de SPAMers e assim, oferecer proteção pelo bloqueio de mensagens indesejadas antes mesmo de chegarem à conta de e-mail do usuário, ou seja, no próprio servidor de correio. Estudiosos acreditam que o SPAM é a maior praga da Internet e poderá ser a razão para a rede se tornar inoperante ou desinteressante em um futuro próximo.

Folha – Vale a pena configurar um firewall local em uma rede empresarial ou deixa isso a cargo dos provedores de acesso?
Marcos – Não se deve delegar tal responsabilidade, especialmente para que o firewall atinja seu poder de proteção máximo, ele precisa ser configurado de forma personalizada e o provedor dificilmente conseguira fazer isso. Por outro lado, seria uma imprudência da minha parte indicar um firewall para todo tipo e tamanho de empresa. Na segurança a regra do custo beneficio também vale e lembre-se, o nível de risco tolerável varia de empresa para empresa e assumir o risco de deixar o controle do firewall com terceiros pode ser a melhor opção para certo grupo de empresas.
Lembre-se que como em qualquer investimento, a segurança também tem que dar retorno, por isso, estudar e conhecer os custos e benefícios de uma solução de segurança antes de adotá-la é racionalmente fundamental e questão de sobrevivência para o responsável pela decisão.

Folha – A segurança da informação hoje é um privilégio das empresas ou o usuário doméstico também pode e deve se preocupar?
Marcos – Deve. Não consigo ver usuário domestico como se fosse uma ilha. De alguma forma ele e parte do sistema de proteção de alguma empresa. Se esse usuário trabalha, ele já é parte da segurança da empresa onde trabalha. Mas se for um aposentado, como correntista de um banco e usuário de seu Internet Banking, ele também é parte do sistema de proteção do banco. Por tudo isso, ele precisa adotar mecanismos de proteção como antivírus, detector de intrusos, anti SPAM, firewall, que reduzam sua exposição e o risco de se tornar uma ponte de falha dele para a empresa de seu relacionamento.

Folha – Um bom jeito de combater os ladrões de informação hoje seria através da Biometria?
Marcos – Sem duvida o processo de autenticação é um dos pontos mais críticos da segurança da informação, por isso, fortalecer este processo significa aumentar rapidamente o nível de segurança de empresas e usuários. A biometria é uma tecnologia moderna e conceitualmente muito mais forte do que as tradicionais técnicas de autenticação baseadas em senha. Tem custo incomparavelmente alto, por isso, mais uma vez a analise da relação custo beneficio precisa ser considerada.

Folha – Explique melhor um pouco de Biometria?
Marcos – O conceito é baseado na comparação de dados biométricos (fornecidos por seu corpo) previamente armazenados em um sistema, com os dados fornecidos pelo seu corpo no momento da autenticação. Pode ser a leitura da íris, da impressão digital, a geometria das mãos, geometria da face, reconhecimento de voz etc. Muitos aspectos a tornam mais fortes que a tradicional senha baseada no conceito "o que você sabe". A biometria usa o conceito "o que você é". Por exemplo, diferente do que ocorre com a senha, você não pode esquecer sua íris em casa, emprestá-la para um amigo ou ser forçado a entregá-la a um ladrão.

"Acredito que veremos uma maior adoção de biometria para autenticação e soluções de gerenciamento"

Folha – Você acha que os riscos em segurança tendem a aumentar muito em 2006?
Marcos – Sim. O risco e o resultado da existência de vulnerabilidades (falhas), ameaças e a probabilidade de uma explorar a outra. À medida que as empresas geram mais informação em meio eletrônico....à medida que as empresas se tornam mais conectadas através de inúmeros meios (wireless, voz sobre IP, Internet, acesso remoto, e-mail, fax...), e ao mesmo tempo, à medida que o conhecimento hacker se desenvolve e dissemina com maior velocidade, o risco tende a aumentar.

Folha – O que podemos esperar de novidade em segurança para o novo ano?
Marcos – Acredito que veremos uma maior adoção de biometria para autenticação, soluções de gerenciamento de identidades, antivírus,firewall, IDS, anti SPAM e filtros de rede de uma maneira geral, operando de forma mais integrada e maximizando os resultados. Alem disso, acredito em modelos mais maduro de governança de riscos considerando novos processos de auditoria, conformidade, contingência, conscientização do usuário e o acompanhamento de indicadores de segurança para apoiar a justificar as iniciativas e investimento em segurança da informação.