Risco digital exige atenção redobrada

Pesquisa com 550 executivos de multinacionais mostra o principal temor das companhias. Segurança da informação é o segundo maior motivo de preocupação

» OSNI ALVES

DIVULGAÇÃO

Sanches: falta confiança na identificação de brechas de segurança

Pelo segundo ano consecutivo, os riscos digitais aparecem como uma crescente preocupação para gestores de alto escalão de diversas empresas ao redor do mundo. É o que indica uma pesquisa da FTI Consulting e Corporate Board Member sobre tendências de questões legais e de governança corporativa. Segundo a pesquisa, realizada com 550 executivos de multinacionais, apenas 32% dos diretores jurídicos e 22% dos diretores executivos acreditam que suas empresas tem capacidade de identificar rapidamente ataques digitais e saber com precisão se informações confidenciais foram comprometidas. O estudo apontou a preocupação com segurança da informação como o segundo principal motivo em ambos os grupos.

O custo médio anual do cybercrime atingiu US$ 8,9 milhões em 2012, segundo dados do Ponemon Institute. Para o diretor sênior e co-líder de risco global e práticas de investigações da FTI Consulting, Michael Pace, com a crescente preocupação com compliance (cumprimento de leis e regulamentos externos e internos), principalmente para as empresas de capital aberto, o uso das mídias sociais tem se tornado um problema real. Apesar de se tratar de um meio que as empresas não podem ignorar, segundo seus diretores executivos, 21% das empresas não têm política de compliance específica para o uso deste recurso. Já 38% não sabia responder a pergunta.

De acordo com o coordenador de cibersegurança da Módulo Security Solutions, Tiago Vilas Bôas, não existe formula mágica, porém, o item mais importante é identificar quais são as ameaças as quais a organização está exposta e, por meio dessas possíveis ameaças, identificar os riscos e as vulnerabilidades. "Uma organização segura é aquela que tem conhecimento das ameaças, riscos e vulnerabilidades e sabe administrá-las conforme a necessidade do negócio", diz.

Para Tiago, que faz pós-graduação em criptografia pela Universidade Federal Fluminense (UFF) e mestrado em Modelagem Matemática pela MAP/FGV, existem algumas ações que necessitam de atenção redobrada, como exposição em mídias sociais (reputação), indisponibilidade da operação e roubo e divulgação de informações confidenciais.

O diretor executivo de segurança da informação e forense digital da FTI, Eduardo Sanches, ressalta que o recente ataque a bancos, considerado o maior da história, realizado em 26 países e com mais de US$ 45 milhões roubados, reflete a falta de confiança dos executivos sobre a capacidade que suas empresas têm para identificar rapidamente brechas de segurança. "Em ambos os grupos pesquisados, menos de um terço é bastante confiante nesta capacidade", acrescenta.

"Em um momento onde os meios digitais (internet e telefonia móvel) são os principais recursos para a realização de transações bancárias, representando 42% do total, passando os meios tradicionais (agências, caixas eletrônicos e contact centers) em 1 ponto percentual, é preocupante saber que pelo menos R$ 95 de cada R$ 100 roubados ou furtados de bancos são decorrentes de fraudes eletrônicas, gerando um prejuízo de R$ 1,4 bilhão de reais", afirma.

Antimalware

Outra pesquisa encomendada, agora pela Kaspersky Lab, fornecedor privado de soluções de proteção de endpoints, e realizada pela agência de análises B2B International no fim de 2012, informa que 82% das empresas no mundo contam com proteção antimalware e 80% usam tecnologias antispam. Como, no entanto, os criminosos virtuais usam técnicas cada vez mais sofisticadas para roubar informações, são necessárias ferramentas adicionais de proteção.

Para os especialistas da Kaspersky Lab, uma média aproximada de 200 mil novos programas maliciosos são enviados diariamente. Além disto, 72% de todas as mensagens de email são spam, o que significa dizer que as soluções que oferecem proteção contra essas ameaças são essenciais, não sendo surpresa que mais de 80% das empresas as adotaram.

Por outro lado, pode-se afirmar que os criminosos virtuais melhoram a qualidade dos códigos maliciosos, além de produzirem malware em grandes quantidades. Em 2012, grandes empresas enfrentaram tentativas de ataques direcionados contra suas infraestruturas de TI.

Nesses ataques, criminosos virtuais usam todos os métodos disponíveis, incluindo técnicas de engenharia social e ataques utilizando exploits, programa que explora sistemas vulneráveis, além de vulnerabilidades ainda desconhecidas. Muitas dessas ferramentas também são usadas em ataques sofisticados e em massa contra usuários domésticos.

As tecnologias tradicionais não são projetadas para oferecer proteção contra códigos maliciosos complexos ou ataques direcionados. O nível de segurança necessário deve ser alcançado somente com o uso de proteções adicionais e com a restrição de atividades que não sejam diretamente relacionadas ao trabalho dos funcionários.

Nesse sentido, os resultados do estudo realizado pela B2B International não são reconfortantes: apenas pouco mais de um terço dos pesquisados criptografa dados corporativos; somente 43% usam sistemas que detectam ataques à infraestrutura de TI (IPS/IDS), e 15% não estão cientes da existência desses sistemas ou não têm interesse em usá-los.

Menos da metade das empresas pesquisadas controlam o uso de dispositivos externos ou de aplicativos de terceiros; e apenas 55% usam a tecnologia de controle de acesso à rede (NAC - Network Access Control). Ao mesmo tempo, há uma tendência positiva: cerca de um quinto das empresas pesquisadas planejam implementar uma ou mais das tecnologias citadas acima ainda este ano.

Anúncio

Fonte: Jornal do Commercio, Rio de Janeiro, 25 jun. 2013, Seudinheiro, p. B10.