A disseminação dos seguros em segurança digital pode estar fornecendo uma sensação inadequada de falsa segurança ao setor de Serviços Financeiros. Recente Relatório e Análise de Serviços Financeiros em 2015, realizado pela Raytheon Websense indica que os bancos com apólices de seguros digitais não estão necessariamente corrigindo seus problemas de segurança. Em vez disso, confiam nas apólices como administração dos riscos de responsabilidade financeira.

Mesmo assim, o estudo mostra que esse pressuposto é falho: os seguros de segurança digital têm cobertura limitada e só restringem parcialmente o impacto financeiro de um ataque digital de pior cenário. O relatório aponta que 80% dos bancos informaram que contrataram algum seguro de segurança digital.

Valores

Segundo artigo no "Wall Street Journal", comentários do CEO da seguradora norte-americana AIG sugerem que o montante máximo segurado por um banco é US$ 400 milhões. A maioria das apólices de segurança digital tem um valor máximo na faixa de US$ 100 milhões a US$ 200 milhões.

Já um relatório recente da Standard & Poor's observou que se os ataques bem-sucedidos e financeiramente danosos aumentarem, o custo dos seguros poderia subir ou a disponibilidade poderia ser restrita. No pior caso, a frequência e o impacto dos ataques poderiam significar que algumas empresas ou setores seriam considerados não seguráveis, o que os tornaria financeiramente muito mais vulneráveis.

Além disso, o requisito para empresas em serviços financeiros de manter sua conexão em tempo real com a economia global dificulta algumas precauções de segurança lógicas. O mesmo artigo do WSJ relata um estudo recente que sugere que, embora 90% dos bancos criptografem os dados transmitidos, apenas 38% criptografam os dados armazenados. Dos bancos pesquisados, 30% não exigiam autenticação com vários fatores de fornecedores terceirizados.

Vulnerabilidade

Um banco da lista Fortune 500, por exemplo, sabe que vários de seus servidores não receberam patches para um bug grave chamado Heartbleed. O motivo para a falta de remediação para eliminar esta vulnerabilidade, de acordo com o diretor de Segurança de TI do banco (que solicitou ficar anônimo por motivos legais), é que aplicar patches nos servidores interromperia a continuidade com diversos bancos europeus que ainda não atualizaram seus sistemas.

Isso poderia interromper as operações com os parceiros no exterior. Ou seja, as evidências apontam que, cada vez mais, a necessidade da conexão em tempo real com a economia global e os seguros digitais podem prejudicar a eficácia da segurança de TI no setor de Serviços Financeiros.

Em 29 de maio de 2015, a Raytheon Company e o Vista Equity Partners concluíram a operação de joint venture criando nova companhia que combina a Websense, o portfólio da empresa Vista Equity e a Raytheon Cyber Products, uma linha de produtos de Inteligência, Informação e Serviços de Negócios da Raytheon. A recém-formada companhia comercial de cibersegurança será conhecida provisoriamente como a Raytheon|Websense e espera introduzir nova identidade de marca após a conclusão da atividade padrão de integração organizacional.

Fonte: Monitor Mercantil, em 23.09.2015.