Barreiras de comunicação, sistemas de segurança ineficientes e carência educacional dos funcionários têm comprometido a segurança das corporações, afirma estudo global da Websense

Os desafios de comunicação entre profissionais de segurança de TI e executivos, o desejo de reformular os atuais sistemas de segurança e o conhecimento limitado sobre segurança entre os executivos e funcionários têm comprometido a segurança das corporações, segundo o estudo "Obstáculos, Renovação e Aumento da Educação em Segurança", realizado pelo Instituto Ponemon a pedido da empresa de segurança Websesnse.

O levantamento com quase 5 mil profissionais de segurança em TI em 15 países, incluindo o Brasil, revela uma lacuna em relação a conhecimento e recursos nas empresas, elevando o nível de vulnerabilidade e risco de violações nos dados corporativos. No Brasil, a pesquisa ouviu 392 profissionais de TI e segurança de TI.

"Não é surpresa que tantos profissionais de segurança estejam decepcionados com o nível de proteção de suas atuais soluções, uma vez que muitas empresas ainda utilizam soluções legadas que não conseguem barrar a cadeia de ameaças e impedir o roubo de dados", afirma John McCormack, CEO da Websense.

Os resultados revelam um consenso global de que as organizações devem corrigir a lacuna de comunicação entre as equipes de segurança e executivos para melhor proteção contra ataques avançados e o roubo de dados, e investir mais na educação dos funcionários.

Infelizmente, o Brasil aparece acima da média na maioria dos pontos analisados em relação à tecnologia, comunicação e educação em segurança. Confira.

Educação:

@ 52% das empresas não oferecem educação em cibersegurança aos funcionários, com apenas 4% planejando fazê-lo nos próximos 12 meses. (Brasil 58% e 10%, respectivamente)

@ Menos da metade (42%) dos profissionais de segurança de TI passou por um processo de treinamento em ameaças cibernéticas em sua atual função. Daqueles que passaram pelo processo, quase todos (94%) consideraram isso importante em termos de gestão dos riscos virtuais. (Brasil 23% e 92%, respectivamente)

@ Profissionais de segurança acreditam que os três eventos principais que obrigariam as equipes executivas a destinar mais dinheiro às iniciativas de cibersegurança são: roubo de propriedade intelectual (67%), violação envolvendo dados de clientes (53%) e perda de receita em virtude do tempo de inatividade do sistema (49%). (Brasil 75%, 46% e 57%, respectivamente)

Comunicação:

@ 31% das equipes de segurança de TI nunca comentaram com os executivos da empresa sobre questões de cibersegurança. (Brasil 36%)

@ Dos que conversaram, quase um quarto (23%) admite que a frequência foi anual, e outros 19% semestralmente. Apenas 11% responderam trimestralmente e 1% com frequência semanal. (Brasil 22% anualmente, 18% semestralmente e 1% semanalmente)

@ Apenas 38% acreditam que suas empresas investem o suficiente em pessoal e tecnologias qualificadas a fim de atingir eficácia na execução dos objetivos e missão da segurança virtual em suas empresas. (Brasil 42%)

Tecnologia:

@ 29% dos entrevistados reformulariam completamente os atuais sistemas de segurança de suas empresas caso possuíssem os recursos e a oportunidade. (Brasil 31%)

@ Quase metade (47%) se sentiu desapontada com frequência com o nível de proteção que acabou sendo oferecido por uma solução de segurança adquirida. (Brasil 61%). Somente 12% nunca se sentiram decepcionados com suas soluções de segurança. (Brasil 4%)

@ 56% acreditam que uma violação de dados provocaria uma troca de fornecedores de segurança. (Brasil 55%)

@ APTs e ataques de roubo de dados são os principais receios dos profissionais de segurança de TI. (Brasil idem)

@ Mais encorajador é que 49% dizem estar pensando em realizar investimentos e ajustes significativos em suas defesas de cibersegurança durante os próximos 12 meses. (Brasil 61%)

“Ameaças avançadas persistentes e ataques de roubo de dados são os principais receios dos profissionais de segurança de TI”, disse Dr. Larry Ponemon, presidente e fundador do Instituto Ponemon. “Estes temores se manifestam em razão de acreditarem que sua tecnologia necessita de uma reformulação e pela crescente lacuna no compartilhamento de conhecimento e recursos entre os profissionais de segurança em TI e pessoal executivo. É fato encorajador que a pesquisa tenha revelado planos de investimento em tecnologia e educação para o futuro”, completa.

Uma versão completa do relatório, incluindo a metodologia do levantamento, resultados consolidados e taxas individuais de resposta por país estão disponíveis aqui. Para saber como a Websense oferece os recursos mais avançados do mercado em identificação de ameaças, por favor, visite www.websense.com/triton.

Fonte: CIO, em 06.08.2014.