

Por Cleber Marques (*)

Pesquisa realizada em 11 países pela consultoria inglesa Vason Bourne, e divulgada em 2015, mostra que há uma tendência global dos funcionários ignorarem os riscos relacionados à cibersegurança no trabalho. Embora a pesquisa não tenha abordado o Brasil, os dados dos nossos usuários também são alarmantes. Um estudo da Intel, por exemplo, divulgado também ano passado, mostrou que ao menos 46% dos brasileiros desconhecem os riscos de segurança, relacionados à engenharia social, uso de serviços pessoais via web, e uso de dispositivos pessoais no ambiente de trabalho.

O estudo realizado pela empresa inglesa revela que, comportamentos de risco considerados óbvios, como usar novas aplicações sem o consentimento da área de TI, abrir e-mails não solicitados de usuários desconhecidos e até a navegação em sites de conteúdo adulto, são práticas comuns no escritório.

Em Cingapura, 37% dos entrevistados usaram novas aplicações sem permissão da TI, comparado com 33% no Reino Unido e 30% no México. Além disso, cerca de 29% dos funcionários chineses disseram abrir anexos de usuários não verificados, ainda que 72% vejam isso como um risco sério. Nos Estados Unidos, mais de 80% sabem do perigo de abrir anexos de e-mails não solicitados e 17% têm esse tipo de comportamento.

Se até os próprios profissionais de segurança podem ser imprudentes em algumas situações, será que os treinamentos em segurança são uma abordagem eficaz para reduzir os incidentes causados por falhas do funcionário “médio”? Tudo indica que sim.

Quando oferecido em pequenas unidades e continuamente avaliado, o conhecimento obtido por meio de treinamentos pode ser a diferença na criação de uma cultura corporativa de segurança, gerando engajamento de funcionários de todos os níveis.

Ataques simulados

O phishing é um assunto fácil para um treinamento de segurança inicial. Segundo o último relatório da Verizon sobre violações de dados, o phishing foi responsável por 25% de todas as violações registradas. De acordo com uma pesquisa do Ponemon, os ataques de phishing custam, em média US\$ 3,7 milhões ao ano a empresas com cerca de 10 mil funcionários.

A pesquisa do Ponemon ainda mostrou que os treinamentos antiphishing estão longe de ser um desperdício. Segundo o instituto, os programas menos efetivos foram capazes de trazer um retorno de sete vezes o investimento inicial, mesmo contando a perda de produtividade do funcionário devido ao tempo de dedicação ao treinamento.

Uma boa maneira de motivar os funcionários a fazer o treinamento é simular um ataque de phishing. Assim, além de oferecer uma estimativa da frequência com que e-mails de phishing são abertos, os funcionários podem ver o quanto são vulneráveis, gerando um instantâneo engajamento.

Além dos treinamentos de phishing, pode haver módulos sobre como classificar dados, o que pode ser enviado por e-mail e o que pode ser armazenado na nuvem. Existem também treinamentos específicos, como cursos para lidar com informações pessoais de saúde, segurança física, engenharia social, uso das redes sociais e vários outros tópicos.

Portanto, além do investimento em ferramentas e sistemas, é preciso também conscientizar o usuário sobre o impacto que o seu comportamento pode trazer em termos de segurança. Não é à toa que as táticas mais recentes utilizam engenharia social no sequestro e captura de dados da empresa. Infelizmente, ainda não existe um botão que exclua o fator humano do risco.

(*) **Cleber Marques** é diretor da Ksecurity.

Fonte: [CIO](#), em 10.02.2016.