Conscientização: convencendo o board

O ser humano é imperfeito e todos nós erramos. Isto posto, não é de se espantar que, de acordo com uma pesquisa efetuada em 2014 pela IBM, foi constatado que 95% dos incidentes de segurança da informação foram causados por erro humano. Quem trabalha com segurança da informação certamente sabe que, muito mais do que um problema de tecnologia da informação (TI), os crimes cibernéticos são uma questão de condicionamento do comportamento humano.

Eis, então, a importância de investir em um programa de conscientização robusto, contínuo e que transforme seus colaboradores em uma linha de frente de defesa contra as ameaças.

Há, contudo, um porém: como convencer o board de diretores a investir nessa área? Como fazê-los entender que de nada adianta gastar rios de dinheiro com soluções automatizadas e proteção de endpoint se o fator humano não estiver devidamente pronto para identificar ameaças, reportá-las e se tornar o principal “antivírus” do ambiente corporativo?

HACK3R_
RANGER5

HACK3R_
RANGER5

Investimentos desiguais

Embora as empresas de médio e grande porte estejam, aos poucos, entendendo a necessidade de se investir em segurança da informação, tais esforços ainda se concentram unicamente em soluções de segurança como antivírus, firewalls, plataformas de virtualização e assim por diante. Parte disso advém do fato de que o board de diretores não compreende a importância do fator humano dentro de um ambiente corporativo seguro, tampouco o fato de que segurança da informação não é algo necessariamente atrelado ao setor de tecnologia da informação (TI).

Com isso, fica difícil justificar novos investimentos em campanhas de conscientização. Como convencê-los?

"O board precisa entender que segurança da informação é um problema humano."

Não é uma tarefa fácil. Porém, é preciso se esforçar para se comunicar de forma clara e “falar a língua” do board, mostrando como o crime cibernético cresce a cada dia e como a conscientização do fator humano pode reverter uma série de danos financeiros e reputacionais.

Uma boa estratégia é demonstrar os crescentes prejuízos ocasionados pelo crime cibernético — perda de confiabilidade perante o público, multas por desrespeito às legislações de proteção de dados, custos de recuperação pós-incidente, danos na reputação e eventuais custos a serem restituídos ao cliente. Estima-se que, em 2021, o crime cibernético custará US$ 6 trilhões a nível global. Demonstrar como esses custos se diluem em diferentes setores comerciais pode ser uma boa estratégia.

Em seguida, temos que abordar as tendências dos crimes digitais: a maior parte deles se baseia na exploração do fator humano.

Quer mais argumentos? Um incidente cibernético pode afetar o preço das ações de uma empresa pública e até mesmo causar demissões de profissionais *C-level*. É crescente o número de CISOs, CEOs e outros profissionais de alto escalão que perdem seus cargos devido a episódios de segurança cibernética que causam prejuízos de milhões de dólares ao empreendimento.

O mais importante, porém, é deixar bem claro para o board que segurança da informação não é uma questão de TI, mas, sim, uma mudança cultural que permeia todos os níveis hierárquicos de uma empresa. É uma questão de postura, atitude e comportamento.

HACK3R_
RANGER5

Uma vez que o board esteja convencido a respeito da importância de programas de conscientização, vale a pena citar seus benefícios. Seus colaboradores se transformam em uma verdadeira força-tarefa: uma linha de frente capaz de identificar, reportar e se esquivar de eventuais ataques de segurança cibernética.

Mas, é óbvio, jamais devemos nos esquecer de prestar contas. Para o board da diretoria, é importantíssimo ter certeza de um bom retorno sobre o investimento (ROI), o que pode ser demonstrado com métricas claras sobre os impactos do programa no condicionamento do comportamento seguro dos colaboradores.

Tudo isso deve ser repassado de forma acessível e amigável: lembre-se de que você está se comunicando com pessoas não-técnicas, logo, evite jargões, termos e palavras específicas de profissionais do setor.

"Seus colaboradores se transformam em uma verdadeira força-tarefa."

HACK3R_
RANGER5

Bibliografia

Selling security awareness training to your board (The Defence Works, 18 de dezembro de 2018)

Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021 (Cybersecurity Ventures, 13 de dezembro de 2018)