KnowBe4

Neoway
Uma empresa B3

ESTUDO DE CASO

Neoway e KnowBe4 — a Criação de uma Cultura de Segurança

A Neoway é uma organização de tecnologia B2B importante na América Latina. Essa organização brasileira é líder de mercado com sua plataforma de IA e análise de Big Data, trabalhando com clientes de mais de 20 setores, incluindo automotivo, de finanças, de bens de consumo, de petróleo e gás, de tecnologia e outros. A organização percebeu a importância de criar uma cultura de segurança entre seus funcionários.

Uma Oportunidade para Tornar Estratégica a Segurança

Em 2018, a Neoway tinha 400 funcionários, e sua pequena equipe de Segurança de informações (InfoSec) reportava-se ao departamento de engenharia. Apesar de ter centenas de funcionários e estar em uma trajetória de crescimento, a Neoway operava, em alguns aspectos, como uma startup.

A equipe de InfoSec sabia da necessidade de mudar. Por ser uma organização de tecnologia B2B conhecida, com uma força de trabalho em crescimento que, muitas vezes, operava fora de suas funções específicas, a equipe de InfoSec estava preocupada com a possibilidade de a Neoway ser alvo de ataques cibernéticos, principalmente e-mails de phishing. A equipe de InfoSec foi estrategicamente transferida da equipe de engenharia e passou a se reportar diretamente ao CEO. A Neoway também contratou profissionais de segurança talentosos, incluindo Flavio Costa, Diretor de segurança de informações (CISO) da organização, para ajudar a posicionar os programas de segurança da Neoway como fatores críticos de negócios. Uma de suas primeiras tarefas foi implementar um programa de treinamento de conscientização em segurança.

"A plataforma da KnowBe4 era extremamente sofisticada, personalizável e acessível, exatamente o tipo de programa que queríamos implementar."

"Aqui, temos um espírito empreendedor. Se há trabalho a ser feito, as pessoas se empenham para realizá-lo, independentemente do cargo que ocupam", afirmou Costa. "Isso nos proporciona agilidade e eficiência, mas também abre as portas para alguns riscos."

Neoway

Setor

Plataforma de tecnologia de IA e Big Data

Sede

Florianópolis, Brasil

Desafio

O crescimento da empresa fazia com ela fosse alvo de ataques cibernéticos. Além disso, havia a necessidade de mudar de uma mentalidade de startup para uma cultura estratégica de segurança.

Os Números do Sucesso

- Treinamento mensal, inclusive a visualização dos novos episódios de "The Inside Man"
- Centenas de testes de phishing mensais
- Redução da porcentagem de Phish-prone em toda a organização de 20% para 3%
- A proporção de cliques e denúncias mudou de 150:10 para 6:300, mostrando que os funcionários melhoraram a habilidade de identificar e-mails de phishing e denunciá-los à equipe de InfoSec
- Redução dos custos em geral, pois não há mais pagamento por campanha

No início, a equipe de InfoSec contratou a El Pescador, um fornecedor de treinamento de conscientização em segurança com o qual eles já haviam trabalhado antes.

A KnowBe4 Proporciona Poder e Controle

Foi o momento certo para a Neoway. Quase imediatamente depois de ser contratada, a El Pescador foi adquirida pela KnowBe4, fazendo com que a Neoway fosse o primeiro cliente da KnowBe4 no Brasil.

A experiência com a El Pescador tinha sido muito boa, e Costa ficou satisfeito com a transição para a plataforma da KnowBe4.

"A conscientização em segurança sempre foi uma questão muito importante na Neoway e precisávamos de uma plataforma de treinamento de conscientização em segurança que nos ajudasse a alcançar nossos objetivos. E a KnowBe4 era essa plataforma", afirmou Costa. "A plataforma era extremamente sofisticada, personalizável e acessível, exatamente o tipo de programa que queríamos implementar."

O programa de conscientização em segurança que Costa e seus colegas criaram tinha como foco mostrar aos funcionários a importância da segurança cibernética para a empresa.

"Era essencial que nossa força de trabalho entendesse que proteger a empresa contra ameaças cibernéticas era algo importante para o sucesso geral da empresa e que todos nós precisávamos participar desse processo", disse Costa.

"Como tínhamos muito controle sobre como e quem testávamos com a KnowBe4, aprendemos muito sobre os hábitos de nossos funcionários."

Costa implementou um treinamento robusto de conscientização em segurança e um programa de simulação de phishing para testar os funcionários com e-mails de phishing usando quatro tipos diferentes de mensagens: mensagens dos sistemas da Neoway, como o G Suite, mensagens do departamento de RH ou da gerência, e-mails de organizações parceiras conhecidas e e-mails de phishing contendo tópicos genéricos. Também foram realizados testes com diferentes tipos de campanhas de phishing em diversos departamentos.

"Como tínhamos muito controle sobre como e quem testávamos com a KnowBe4, aprendemos muito sobre os hábitos de nossos funcionários e sobre o que despertava o interesse deles em clicar", afirmou Costa. "Os e-mails simulados de phishing do nosso departamento de RH e de nossos sistemas internos, como o G Suite, foram os que tiveram mais cliques das pessoas. Foi ótimo ter uma ideia do que motivava um funcionário a clicar."

Sabe o que também foi muito importante? Costa percebeu que os funcionários não estavam denunciando quando suspeitavam de um link ou e-mail fraudulento.

Costa continuou: "Conseguimos ver que somente 10% dos funcionários estavam usando o Phish Alert Button para denunciar a situação à nossa equipe de InfoSec. Com essa informação, conseguimos incorporar a nossos treinamentos a importância de denunciar e-mails suspeitos."

Decisões bem Fundamentadas com o PhishER

Com a implementação de um programa robusto de conscientização em segurança, que treina os funcionários mensalmente e realiza testes simulados de phishing várias vezes por semana, Costa estava pronto para seguir por uma direção ainda mais avançada.

"Ensinamos nossos funcionários que denunciar um e-mail suspeito... era algo que eles poderiam fazer para melhorar a integridade da nossa organização."

"Ensinamos nossos funcionários que denunciar um e-mail suspeito, seja um e-mail de phishing real ou um teste simulado da KnowBe4, era algo que eles poderiam fazer para melhorar a integridade da nossa organização", disse Costa. "No entanto, com o passar do tempo, houve ocasiões em que 300 funcionários denunciaram algo ao nosso departamento de InfoSec, o que é ótimo, mas também muito desgastante."

Foi quando a Neoway incorporou o **PhishER**, uma plataforma leve de orquestração, automação e resposta de segurança (SOAR) que gerencia o alto volume de mensagens de e-mail potencialmente maliciosas denunciadas pelos usuários.

De acordo com Costa, "com o PhishER, a equipe de InfoSec pode ser mais criteriosa. Ele coloca os e-mails denunciados em uma fila e prioriza esses e-mails para nós, o que nos possibilita lidar com os mais importantes primeiro. Com isso, conseguimos ter mais eficiência e proteger melhor nossa organização, mantendo o foco nas mensagens que representam uma ameaça maior."

Para que o departamento de InfoSec se tornasse uma divisão estratégica de negócios, Costa também introduziu o **Virtual Risk Officer** (VRO) da KnowBe4 na Neoway.

"A KnowBe4 nos ajudou a treinar nossos funcionários e, depois, a testá-los. O PhishER facilitou o processo de denunciar as ameaças e nos ajudou a avaliar melhor a integridade de nossas redes em relação às ameaças de phishing", afirmou Costa. "A inclusão do VRO da KnowBe4 foi uma decisão estratégica que nos ajudou a obter uma compreensão melhor e mais detalhada da nossa postura de risco."

Com o VRO, a Neoway conseguiu obter informações detalhadas em formato de painel para ilustrar o risco que indivíduos, departamentos, funções e grupos representam. Como os funcionários estão sendo treinados e testados o tempo todo, seus níveis de risco aumentam e diminuem, proporcionando a Costa e à equipe de InfoSec a oportunidade de identificar a necessidade de remediação em uma área específica.

"A inclusão do VRO da KnowBe4 foi uma decisão estratégica que nos ajudou a obter uma compreensão melhor e mais detalhada da nossa postura de risco e a proteger ainda mais a nossa empresa."

Criação de Conscientização, Comportamento e Cultura

Costa implementou um programa criterioso de treinamento de conscientização em segurança. Mas, como a KnowBe4 é a fonte oficial de cultura de segurança, eles complementaram esse programa com outro objetivo.

"A KnowBe4 nos apresentou aos especialistas em cultura de segurança deles, o que foi um divisor de águas para nós."

"Inicialmente, queríamos que nossos funcionários aprendessem a proteger a organização contra ameaças de phishing, algo que a KnowBe4 nos ajudou a alcançar. Entretanto, a parceria com a KnowBe4 nos proporcionou benefícios muito além do esperado", afirmou Costa.

"A KnowBe4 nos apresentou aos especialistas em cultura de segurança deles, o que foi um divisor de águas para nós. Até onde sei, Perry Carpenter, da KnowBe4, é a pessoa mais importante hoje em dia quando o assunto é segurança de informações, pois ele é uma autoridade que transforma a maneira como as pessoas veem a segurança, identificando seus comportamentos em relação a ela e entendendo a reação das pessoas", disse Costa. "Graças à KnowBe4, mudamos o nome do que fazemos. O que fazemos não é simplesmente seguir um programa de segurança. Nós seguimos um programa de cultura, comportamento e conscientização em segurança."

Costa sabe que uma organização nunca está totalmente segura. Mas, graças à **plataforma de treinamento de conscientização em segurança e de simulação de phishing da KnowBe4,** ao PhishER e ao VRO, ele sabe que está fazendo tudo o que é possível para proteger os ativos digitais da Neoway.

"Como a KnowBe4 nos ajudou a entender por que a cultura de segurança é tão importante, criamos uma base cultural muito exclusiva e estável que beneficia significativamente nossa organização", declarou Costa.