KnowBe4
Human error. Conquered.

Considerações importantes ao avaliar fornecedores de treinamentos de conscientização em segurança

Considerações importantes ao avaliar fornecedores de treinamentos de conscientização em segurança

Sumário

Introdução 2

Avaliação de plataformas de treinamento de conscientização em segurança 2

Sete componentes essenciais que um fornecedor de SAT deve oferecer 3

1 - Conteúdo variado e envolvente 3

2 - Localização 4

3 - Estrutura e automação 4

4 - Testes 4

5 - Métricas e relatórios 5

6 - Pesquisas e avaliações 6

7 - Muito mais do que o SAT 6

Lista de verificação para fornecedores de SAT 7

Conclusão 7

IN T RODUÇ ÃO

O panorama de fornecedores de treinamento de conscientização em segurança (Security Awareness Training, SAT) é diversificado e inovador. Esse mercado mudou muito ao longo dos últimos anos. Hoje, CISOs e líderes de segurança tentam garantir que qualquer programa de SAT mude o comportamento dos usuários e possibilite que todos na empresa consigam compreender, reduzir e monitorar os riscos cibernéticos dos funcionários.

Um fornecedor de SAT deve oferecer uma plataforma para alcançar esses objetivos ao:

- Ajudar a desenvolver uma mentalidade mais ampla quanto à cultura de segurança e ao gerenciamento de riscos gerados por falhas humanas
- Fornecer as ferramentas necessárias para promover e mensurar mudanças no comportamento
- Garantir que os usuários se tornem o firewall humano de sua organização e a última linha de defesa contra ataques cibernéticos e violações de dados.

Este documento informativo fornece uma visão geral das considerações que devem ser feitas antes de se avaliar plataformas de SAT e, o mais importante, apresenta sete componentes essenciais que qualquer fornecedor de SAT deve oferecer para ajudar a organização a alcançar as metas.

AVALIAÇÃO DE PLATAFORMAS DE TREINAMENTO DE CONSCIENT EM SEGURANÇA

Muitos programas de SAT antigos não consideram aquilo que chamamos de lacuna de conhecimento-intenção-comportamento. Resumidamente, o simples fato de fornecer aos usuários informações e dados a respeito da conscientização em segurança não significa que esses usuários aprenderão com isso ou passarão a se preocupar com essa questão.
Sozinhas, as informações não mudam as ações. Basicamente, os indivíduos serão atraídos a seguir um caminho de menor resistência ou habitual. É importante que as principais partes interessadas em sua organização entendam estas três realidades antes de avaliar um fornecedor de SAT.

- **Fazer com que alguém se conscientize não significa que essa pessoa vai se importar**
  Disponibilizar um enorme volume de informações, dados e procedimentos aos funcionários não fará com que eles se importem com a conscientização em segurança. Ao receber uma recomendação de segurança, a maioria dos funcionários levará isso em conta e analisará essa recomendação em relação a outras prioridades.

- **Se você tentar ir contra a natureza humana, o fracasso será certo**
  Se houver uma lacuna entre as expectativas das suas políticas e a realidade de comportamento mencionada anteriormente, seu programa de SAT provavelmente ficará muito abaixo das expectativas. Afinal de contas, você está fornecendo treinamento para seres humanos e definindo expectativas para eles, e não programando dados em um computador.

- **O que os funcionários fazem é muito mais importante do que eles sabem**
  Sozinho, o conhecimento nunca impediu que uma violação ocorresse em uma organização. O comportamento é o elemento que fortalecerá a postura de segurança de uma organização ou que resultará em uma violação. Concentre-se no comportamento, e não apenas no fornecimento de informações e na apresentação de políticas.

SETE COMPONENTES ESSENCIAIS QUE UM FORNECEDOR DE SAT DEVE OFERECER

Ao avaliar fornecedores de SAT, verifique se eles oferecem os sete componentes que listaremos a seguir. Isso garantirá o sucesso de um programa de SAT no curto prazo e também no futuro, mostrando todas as possibilidades.

1 - Conteúdo variado e envolvente

O conteúdo é o item mais importante. É o componente informativo de qualquer programa de SAT. Vale lembrar que não há um modelo universal para o conteúdo. Os usuários são atraídos por diferentes estilos de conteúdo que correspondem a suas preferências individuais de aprendizado. Tenha isso em mente ao avaliar as plataformas de SAT. Para mudar o comportamento e criar uma cultura de segurança sólida em sua organização, é essencial ter uma variedade de conteúdos que despertem o interesse de diferentes grupos de funcionários. Procure por uma plataforma de SAT que tenha uma grande biblioteca de conteúdos relevantes em vários idiomas, que seja atualizada continuamente e que inclua módulos interativos, vídeos, jogos, pôsteres, boletins informativos, avaliações etc.

> Assegure-se de que o fornecedor de SAT permita o aprendizado móvel para que os usuários consigam assistir ao conteúdo e fazer os exercícios onde quer que estejam.

Além disso, considere treinamentos com base no cargo ou nas preferências. O que você ensinará às pessoas que trabalham em um call center provavelmente será diferente do que ensinará a alguém da área de TI. O conteúdo deve levar em conta essas diferenças. Em termos demográficos, os usuários terão diferentes estilos de aprendizado dentro de sua organização. Por exemplo: alguns absorverão melhor vídeos engraçados com duração de três a cinco minutos; já uma equipe de executivos pode não se sentir à vontade com esse tipo de abordagem. Ter flexibilidade quanto aos principais temas de treinamento para garantir que todas as pessoas assimilem o conteúdo de que precisam é uma consideração de extrema importância ao avaliar as plataformas de SAT.

Por fim, a implantação do conteúdo de treinamento para os usuários é quase tão importante quanto o conteúdo em si. Assegure-se de que o fornecedor de SAT permita o aprendizado móvel para que os usuários consigam assistir ao conteúdo e fazer os exercícios onde quer que estejam. Além disso, ter uma interface administrativa fácil de usar e que permita não só atribuir, acompanhar e mensurar os esforços de treinamento, mas também gerar relatórios, é fundamental para que você chegue a conclusões úteis e significativas sobre o aumento e a redução dos riscos e saiba quais são os grupos da organização que precisam de mais intervenção. Além disso, procure por plataformas de SAT flexíveis que permitam integrar conteúdos personalizados de terceiros.

2 - Localização

A localização é o processo essencial de traduzir o conteúdo, além de fornecer exemplos, imagens e elementos interativos específicos da região para os usuários. Esse processo detalhado vai muito além da simples tradução de conteúdo e é fundamental para as organizações presentes no mundo todo e que contam com uma base de funcionários que falam vários idiomas.

A parceria com um fornecedor de SAT que possibilite que os usuários selecionem a região em que estão localizados ou o idioma com o qual eles se sentem mais à vontade é um fator importantíssimo para garantir a absorção e o uso do material de treinamento. O fornecedor de SAT deve fornecer localizações de alta qualidade e contar com a ajuda de especialistas locais no assunto para garantir a relevância do conteúdo e dos exemplos.

3 - Estrutura e automação

O SAT não é algo que se faz uma única vez. Criar uma cultura de segurança é algo que exige treinamentos e testes constantes e, depois, reforço. Além disso, ao criar um programa de SAT, lembre-se de que o aprendizado ocorre em três fases diferentes. Por esse motivo, é muito importante procurar por plataformas de SAT que tenham o conteúdo e as ferramentas necessários para manter o foco e fornecer resultados em cada fase.

- **Aprendizado formal estruturado** (**10%)** – refere-se a elementos como treinamento presencial em sala de aula, treinamento on-line implantado por um Sistema de gerenciamento de aprendizado (Learning Management System, LMS), dias de treinamento etc.

- **Aprendizado informal (20%)** – envolve pedir sugestões para outros membros da equipe, colaborar, assistir a vídeos ou ler.

- **Aprendizado prático (70%)** – engloba principalmente oportunidades de aprendizado diário, como a interação social no trabalho e o contato com fluxos de trabalho corporativos ou com a cultura corporativa e do departamento.

90% do aprendizado de uma pessoa ocorre fora de contextos formais estruturados.

Como se pode ver, 90% do aprendizado de uma pessoa ocorre fora de contextos formais estruturados. Muitos programas de SAT não dão certo porque se concentram exclusivamente nesses primeiros 10%. Seu programa de SAT deve englobar as três fases, e as plataformas de SAT que você estiver avaliando devem ter as ferramentas necessárias para cobrir as três fases de aprendizado. Um ótimo exemplo disso seria disponibilizar um pequeno vídeo sobre senhas na página de alteração de senha de sua organização, tornando-o prontamente acessível quando for necessário.

Agora, falaremos sobre automação, que também é muito importante. Qualquer fornecedor de SAT deve incorporar elementos de automação em seu programa para facilitar o provisionamento de usuários, de modo que seja possível agendar campanhas de treinamento com semanas de antecedência sem a necessidade da ação direta dos administradores do programa. Essa automação também facilita o uso e aumenta o ROI ao otimizar o tempo de gerenciamento do programa e fornecer conteúdo com mais eficácia aos usuários certos, no momento certo. A automação também pode ser utilizada para fornecer eventos reativos/com base em correções de "treinamento pontual" e para fornecer relatórios agendados para a gerência e os executivos.

4 - Testes

Embora o treinamento seja o alicerce de qualquer programa de SAT, a aplicação de testes nos usuários para verificar como eles reagem a simulações de phishing é uma forma de determinar se você está mudando o comportamento de segurança e reduzindo os riscos gerados por falhas humanas. O usuário clicará no e-mail, irá denunciá-lo ou não fará nada?

Além disso, os usuários precisam de uma forma simplificada de denunciar e-mails de phishing para ajudar a sua organização a desenvolver resiliência. Com esse mecanismo de denúncia, sua equipe de TI consegue obter mais informações sobre possíveis ataques direcionados à sua organização, além de alertar todas as outras pessoas. Embora a maioria das plataformas de SAT forneça vários tipos de simulações e modelos de phishing, além de ferramentas de usuário final que permitem a denúncia de ataques de phishing, o problema está nos detalhes. Trabalhe com um fornecedor de SAT que esteja à frente do panorama de ameaças e, como resultado disso, forneça modelos de e-mail de phishing com base nas ameaças do mundo real.
Além disso, se um funcionário não passar em um teste simulado de phishing, a plataforma de SAT deverá fornecer um treinamento "pontual" para proporcionar um momento de aprendizado sobre esse incidente específico enquanto isso ainda for algo recente na mente do usuário.
Assim como a entrega de conteúdo e o desenvolvimento do programa, os programas de simulação de phishing também se beneficiam da automação e do aprendizado de máquina. A plataforma de simulação de phishing de um fornecedor deve usar aprendizado de máquina para recomendar e fornecer modelos de phishing personalizados e confiáveis com base no histórico de phishing e treinamento de um usuário, além de ser capaz de reconhecer e-mails de phishing legítimos e transformá-los em testes simulados.

5 - Métricas e relatórios

A mensuração e os relatórios são outra forma de determinar a eficácia do programa de SAT no que se refere à mudança de comportamento e à redução dos riscos gerados por falhas humanas. Esses componentes também são importantíssimos para quantificar o sucesso de seu programa de conscientização em segurança para os executivos.

Conhecer o desempenho do seu programa em relação às metas e aos objetivos e conseguir demonstrar claramente as melhorias são questões essenciais para manter o apoio dos executivos. Um bom fornecedor oferecerá uma plataforma eficiente de relatórios e análises para permitir que a organização mensure tudo o que for mais importante. Isso também deve incluir relatórios executivos para permitir que os gerentes dos programas de SAT criem relatórios com facilidade, personalizados especificamente para a equipe de liderança. Além disso, é importante identificar os fornecedores que mensuram os riscos gerados por falhas humanas e avaliam as métricas de cultura de segurança. As métricas dos programas de SAT mais antigos geralmente se concentram nas taxas de conclusão, no desempenho dos usuários no quiz, nas métricas de engajamento etc. É muito importante conseguir mensurar o perfil de risco de indivíduos ou departamentos para que seja possível tomar decisões baseadas em dados e saber quais ajustes precisam ser aplicados ao treinamento. É necessário conseguir avaliar como os riscos da sua organização mudam ao longo do tempo e mensurar realmente o desempenho do seu programa de treinamento para compreender os pontos que precisam ser melhorados para fortalecer o firewall humano da sua organização.

6 - Pesquisas e avaliações

A existência de treinamentos formais e contínuos de conscientização em segurança pode parecer algo sem sentido para os funcionários, uma vez que eles podem achar que a segurança cibernética é uma tarefa da equipe de TI. Sendo assim, é importante compreender as atitudes existentes em sua organização e a forma como elas mudam com a presença do SAT. Isso ajudará a destacar as áreas em que o desempenho é bom ou em que são necessárias ações de correção. Isso também permite que você avalie o progresso da cultura de segurança, o que é diferente das métricas mencionadas anteriormente, pois você analisará a preferência, a opinião e o estado de espírito das pessoas.

As pesquisas e avaliações devem incluir não só a mensuração de opiniões e atitudes, mas também de conhecimento e proficiência. Qualquer plataforma de SAT deve possibilitar a aplicação de avaliações com base em habilidades e pesquisas sobre cultura de segurança para que seja possível mensurar o conhecimento e a proficiência em segurança dos seus usuários e avaliar a postura geral da cultura de segurança da sua organização. O objetivo é identificar os usuários que consigam responder melhor a uma determinada situação e que saibam o que significa fazer o que é certo. Além disso, as plataformas devem possibilitar a comparação de sua organização com pares no setor e padronizar as avaliações com validade científica para mensurar, com precisão, o progresso que a organização obteve.

Elas também precisam incluir a capacidade de avaliar o nível de riscos gerados por falhas humanas dos funcionários. Lidar com o gerenciamento de riscos gerados por falhas humanas é um objetivo de extrema importância. Quando se compreende o perfil de risco de um indivíduo ou departamento, é possível fazer ajustes no treinamento e obter insights importantes sobre quais pontos do programa de segurança devem ser melhorados, reforçando a postura de segurança da organização.

7 - Muito mais do que o SAT

O cenário de fornecedores de SAT passou por uma grande mudança nos últimos anos. Os principais fornecedores mudaram suas ofertas com foco exclusivo no treinamento dos usuários e passaram a oferecer plataformas que, agora, lidam com questões mais abrangentes, como a criação de uma cultura de segurança em uma organização e o gerenciamento de riscos gerados por falhas humanas.

É essencial trabalhar com um fornecedor de SAT que alcance suas metas imediatas e que também mostre o que é possível fazer no futuro. Tenha estes pontos importantes em mente ao avaliar um fornecedor de SAT:

- **Concentre-se na conscientização, no comportamento e na cultura de segurança**
  Basicamente, sua meta deve ser a de reduzir os riscos gerados por falhas humanas. De acordo com a Forrester Research*, é importante trabalhar com fornecedores que ofereçam cálculos e quantificação de riscos gerados por falhas humanas com base no comportamento dos usuários. Com isso, o SAT passará a ser a base fundamental para moldar sua cultura de segurança.

- **O fornecedor tem um conjunto de ofertas que permitirá que a sua organização vá além do SAT?**
  Como já mencionado anteriormente, o SAT é o alicerce para a criação de uma cultura de segurança em uma organização, mas não é necessariamente o único componente. Outros componentes, como a Human Detection and Response (HDR), as plataformas de SOAR, a resposta a incidentes e a inteligência de ameaças, são igualmente importantes e poderão ser incluídos no seu roteiro de cultura de segurança no futuro. Trabalhe com um fornecedor que atenda a suas necessidades atuais e futuras.

* The Forrester Wave: Security Awareness and Training Solutions, 1º trimestre de 2022

LISTA DE VERIFICAÇÃO PARA FORNECEDORES DE SAT

- ☐ Biblioteca ampla e diversificada de conteúdo de aprendizado
- ☐ Localização
- ☐ Plataforma de treinamento e de phishing altamente automatizada
- ☐ Ofornecedor permite que você envie seu próprio conteúdo de treinamento ou baixe conteúdo da plataforma dele?
- ☐ Plataforma de implantação de treinamento com recursos de automação
- ☐ Capacidade de enviar conteúdo de terceiros para a plataforma de treinamento/LMS
- ☐ Plataforma flexível de simulação de phishing com modelos variados, personalizáveis e localizados
- ☐ Integração de automação, inteligência artificial e aprendizado de máquina às plataformas de treinamento e phishing
- ☐ Recursos eficientes de avaliação e teste de usuários para avaliar o conhecimento dos usuários e o impacto do treinamento
- ☐ Métricas intuitivas e recursos de geração de relatórios para informar o ROI
- ☐ Recursos de geração de relatórios executivos

CONCLUSÃO

Todos esses recursos formam a base para garantir que o programa de SAT da sua organização mude o comportamento dos usuários e possibilite que sua empresa realmente compreenda, reduza e monitore os riscos cibernéticos. O SAT atuará como uma plataforma para promover uma compreensão mais ampla da cultura de segurança e do gerenciamento de riscos gerados por falhas humanas e fazer com que os usuários passem a ser o firewall humano da sua organização.

CLIQUE AQUI

Saiba mais sobre o **Treinamento de conscientização em segurança de Kevin Mitnick** da KnowBe4

Recursos adicionais

Teste de phishing gratuito
Faça este teste de phishing gratuito e descubra qual é a Porcentagem de Phish-prone dos seus funcionários

Automated Security Awareness Program gratuito
Crie um programa de conscientização em segurança personalizado para sua organização

Phish Alert Button gratuito
Agora, seus funcionários podem denunciar ataques de phishing de maneira segura com apenas um clique

Email Exposure Check gratuito
Descubra quais e-mails de usuários estão expostos antes que os infratores façam isso

Domain Spoof Test gratuito
Descubra se os hackers conseguem falsificar um endereço de e-mail no seu domínio

Sobre a KnowBe4

A KnowBe4 é a maior plataforma integrada do mundo de treinamento de conscientização em segurança e simulação de phishing. Reconhecendo que o elemento de segurança humano tem sido seriamente negligenciado, a KnowBe4 foi criada para ajudar as organizações a administrar o problema constante da engenharia social por meio de uma abordagem moderna e completa de treinamento de conscientização.

Esse método integra testes de linha de base que simulam ataques do mundo real, treinamento interativo e envolvente e avaliação contínua por meio de relatórios simulados de integridade corporativa para criar uma organização mais resiliente, que tem a segurança como prioridade.

Dezenas de milhares de organizações no mundo todo usam a plataforma da KnowBe4 em todos os setores, incluindo campos altamente regulamentados, como finanças, saúde, energia, governo e seguros, para mobilizar seus usuários finais como uma última linha de defesa e capacitá-los a tomar decisões mais inteligentes sobre segurança.

Para obter mais informações, acesse: www.KnowBe4.com