SOPHOS

Como realizar um exercício tabletop de segurança cibernética

As melhores práticas de uso de exercícios tabletop para ajudar sua organização a se preparar contra ataques cibernéticos

Documento técnico Sophos. Julho, 2024

Apresentação

Os exercícios tabletop testam a qualidade de operação de uma equipe ou processo através da simulação de uma situação e sua resposta efetiva com base em um plano de ação prévio. Esses exercícios são uma valiosa ferramenta já de grande data usados para se preparar para cenários adversos. As forças armadas realizam exercícios tabletop para aplicar diferentes estratégias em resposta a conflitos; já os governantes os utilizam para melhorar a resposta a crises. Nas organizações, os exercícios tabletop são uma forma eficiente de se preparar contra ataques cibernéticos.

Este guia explica o que são os exercícios tabletop de segurança e como executá-los. Ele se fundamenta na abordagem adotada pela equipe Sophos Cybersecurity para preparar a nossa própria organização contra ataques.

Transparência é a pedra fundamental da filosofia da Sophos, e temos grande prazer em compartilhar nossas estratégias e recursos. Visite nosso Trust Center para mais informações e recursos.

O que é um exercício tabletop de segurança?

Um exercício tabletop engloba um ataque cibernético e seus possíveis danos. Com ele, você saberá como a sua organização se sairá na hora de responder a um ataque, além de ter em mãos insights sobre a segurança cibernética que o ajudarão a aperfeiçoar sua abordagem.

Por que isso é importante?

Identificação de pontos cegos: os exercícios tabletop de segurança ajudam você a identificar pontos cegos na sua segurança cibernética antes que os criminosos cibernéticos possam encontrá-los e explorá-los.

Análise de postura de segurança: com exercícios tabletop de segurança cibernética, você pode avaliar sua postura de segurança e encontrar formas de otimizá-la.

Análise de comunicação: exercícios tabletop de segurança cibernética podem evidenciar problemas de comunicação entre equipes e departamentos que podem interferir na sua capacidade de tratar dos ataques cibernéticos.

Conformidade: conduzir e documentar exercícios tabletop de segurança é um requisito de preparação a incidentes nos programas de segurança de muitas indústrias altamente regulamentadas.

Fluência de resposta: acompanhar as respostas em um incidente simulado permite que os participantes desenvolvam maior fluidez no desempenho de ações necessárias no caso de um ataque real, acelerando sua execução.

Tipos de exercícios tabletop de segurança

Existem vários tipos de exercícios, com diferentes durações e diferentes benefícios.

Cenários rápidos

Um cenário rápido apresenta "um nível extremamente alto para ser entendido e discutido com facilidade e rapidez", de acordo com ISACA. Requer o mínimo de preparo e dura entre 10 a 30 minutos.

Os cenários rápidos, também chamados "rapid-fire", podem incluir equipes integradas por pessoal júnior, intermediário e sênior e com grande diversidade de especialização. Os membros das equipes podem examinar vários cenários de segurança, cada qual atuando como responsável por responder ao incidente.

Cenários técnicos

Os cenários técnicos consomem, em geral, cerca de uma a duas horas. Esses cenários, também chamados "technical-only", promovem discussões técnicas profundas e exigem intenso planejamento. Com eles, os membros das equipes podem avaliar os aspectos técnicos de um incidente de segurança.

Um cenário apenas técnico normalmente envolve um evento de "semeadura". Conforme o evento se desenrola, sua organização pode adicionar mais detalhes a ele. Isso ajuda os membros da equipe a se prepararem para ataques cibernéticos mais complexos.

Cenários completos

Cenários completos são os cenários técnicos expandidos. Eles focam em questões técnicas e problemas diversos e de logística.

Um cenário completo, também chamado "full-stakeholder", dura, em geral, entre duas e quatro horas. Pode incluir membros da equipe técnica, além de profissionais do jurídico, marketing e RH.

Os cenários completos são ideais para as organizações que desejam melhorar a comunicação entre equipes e departamentos. Combinar o pessoal técnico e não técnico em um exercício tabletop completo pode ser bastante benéfico. Isso dá aos participantes de diferentes equipes e departamentos a oportunidade de trabalharem em conjunto para tratar de um problema de segurança.

Algumas organizações solicitam que as equipes e/ou departamentos ingressem no cenário em diferentes momentos. Assim, as equipes e departamentos começam a se envolver gradualmente, do mesmo modo que aconteceria em um incidente de segurança real.

Quem executa um exercício tabletop de segurança?

Os exercícios tabletop de segurança podem ser realizados por equipes internas ou por pessoal externo, oferecendo grandes benefícios para as organizações.

Externo

Os provedores de serviços de segurança tabletop facilitam e gerenciam cenários e levantam pontos de debate. Nesse ambiente, os esforços exigidos de você para instalar e executar o processo são mínimos.

O procedimento típico do provedor externo é adaptar o exercício tabletop à sua organização e ambiente específicos. Normalmente, o provedor se inteira sobre o seu negócio e os desafios com a segurança para então desenvolver um exercício tabletop de segurança personalizado e de acordo com a sua situação.

Interno

Você pode traçar os seus próprios exercícios de segurança. O desenvolvimento e implementação de tabletops por equipes internas pode ser um processo caro e demorado, porém, você pode adaptar totalmente seus exercícios de segurança cibernética à sua organização e ambiente. Por exemplo, alguns desafios podem envolver sistemas que os participantes usam diariamente, tornando-os mais "reais" e estabelecendo um maior engajamento.

Tabletops internos também podem trabalhar em conjunto para identificar e tratar de questões específicas que impactam diretamente a sua organização, funcionários e clientes.

A abordagem da Sophos

Na Sophos, criamos exercícios tabletop de segurança cibernética personalizados para equipes ou departamentos específicos. Em um exercício, normalmente começamos com um pequeno problema de segurança e encorajamos os participantes a compartilhar abordagens e ideias entre eles. A partir desse ponto, usamos "resultados" para ressaltar a gravidade do problema.

Veja abaixo alguns temas para os cenários de segurança cibernética que executamos e que as organizações podem usar para desenvolver e executar seus próprios exercícios tabletop.

EQUIPE	CENÁRIO
Sophos X-Ops	Ameaças internas
RH	Ransomware e vazamento de dados pessoais dos funcionários
Suporte técnico	Ataque direcionado por alguém se passando por um cliente
Marketing	Um funcionário comprometido levando ao aniquilamento do site e das redes sociais da empresa
Legal	Compensação a pesquisadores de bugs maliciosos
Sophos X-Ops	Sistema de análise comprometido, ataque à cadeia de suprimentos
Engenharia	Binários da Sophos comprometidos, ataque à cadeia de suprimentos
Engenharia	Engenharia de phishing
TI	Incidente de ransomware de grande escala
Engenharia	Vulnerabilidade de dia zero em um aplicativo que leva ao comprometimento da base de clientes

Práticas recomendadas para desenvolver um exercício tabletop de segurança

As seguintes práticas o ajudaram a desenvolver exercícios tabletop de segurança eficientes e totalmente voltados a você:

1. Identifique o seu público-alvo

Determine seu público-alvo e então desenvolva seu cenário de segurança cibernética. Por exemplo, um cenário complexo de segurança será o ideal se você estiver testando a sua equipe de segurança cibernética. Entretanto, se você estiver testando sua equipe de TI ou DevOps, opte por um problema que os participantes entenderão e prestarão atenção, dedicando a ele o tempo e a energia devidos.

2. Escolha os participantes certos

Decida se deseja incluir uma única equipe ou departamento, ou vários, em seu cenário de segurança. Um cenário formado por uma única equipe permite que você analise o grau de especificidade com que os participantes responderão a um ataque cibernético. Já um cenário que inclua várias equipes ou departamentos incita as partes envolvidas entre as diferentes unidades comerciais a trabalharem em conjunto para tratar de um incidente de segurança.

3. Decida quando envolver os participantes

Analise e pondere quando as diferentes equipes e/ou departamentos deverão ingressar no seu cenário de segurança cibernética. Por exemplo, se as informações de identificação pessoal (PII) da sua organização forem comprometidas, você precisará envolver membros da sua equipe jurídica para assegurar a conformidade com a regulamentação GDPR e outras obrigações de segurança de dados.

É sempre benéfico incluir pelo menos uma pessoa de cada equipe ou departamento da sua organização em um cenário de segurança. Isso ajuda a fomentar a comunicação e colaboração entre funções.

4. Decida quantos participantes incluir

Assegure-se de que o seu cenário inclua participantes que possam se engajar uns com os outros e trabalhar em colaboração para atingir objetivos comuns. Em nossos cenários, geralmente incluímos até 25 participantes de diferentes níveis de uma única equipe ou departamento, ou várias equipes ou departamentos. Ao decidir quantos participantes incluir em seus exercícios tabletop de segurança, considere o tamanho da sua organização e a estrutura de suas equipes e departamentos.

5. Calcule o tempo do seu exercício

Dê aos participantes tempo suficiente para fazer o exercício tabletop. Na Sophos, tentamos evitar sessões demasiado longas de exercícios tabletop, isso porque pode ser difícil para os participantes coordenar suas agendas e ingressar em sessões que durem mais do que algumas poucas horas.

6. Prepare os seus materiais

Use uma apresentação do PowerPoint ou outros materiais para apresentar o seu cenário. A equipe da Sophos normalmente usa apresentações em PowerPoint para explicar seus exercícios tabletop, em que cada slide mostra a progressão dos eventos e questionamentos que os participantes devem considerar. Normalmente, limitamos o tamanho de nossas apresentações de exercícios em PowerPoint a 20 slides.

7. Crie a sua história tabletop

Desenvolva uma história teórica e adapte as informações nela incluídas conforme desejado. Histórias e notícias mais recentes ajudam a atrair a atenção dos participantes. Para histórias mais extensas, você pode usar breadcrumbs para o rastreamento digital de sistemas e logs dos participantes para localizá-los e acompanhá-los.

8. Correlacione o seu exercício tabletop com os participantes

Crie um exercício tabletop de segurança cibernética com base na maturidade de segurança de seus participantes. Por exemplo, uma história detalhada pode beneficiar os participantes com habilidades e perícia avançada em segurança cibernética. Em outras situações, um cenário genérico de alto nível pode ser o mais indicado.

Se estiver desenvolvendo uma narrativa detalhada, assegure-se de que seja realista. Por exemplo, se quiser atingir uma parte específica da sua organização ou rede, obtenha insights com alguém da área desejada. Dessa forma, você poderá criar um cenário que reflita o seu público-alvo.

9. Obtenha feedback dos participantes

Pergunte aos participantes se têm ideias que você possa incorporar aos seus exercícios. A maioria dos participantes poderá compartilhar insights sobre pontos fracos na segurança que enfrentam diariamente. Você pode usar esses pontos fracos para desenvolver um cenário que ajude os participantes a encontrar formas de tratar esses problemas no futuro.

10. Mapeie o seu cenário

Trace um fluxograma de como o seu ataque simulado se desenrolará. Isso ajuda a encontrar as falhas na sua história. Peça também aos membros das equipes e departamentos que têm entendimento sobre as questões abrangidas na sua história que deem seu feedback. Esses membros de equipes e departamentos podem ajudar você a resolver problemas e garantir que o seu cenário seja realista.

11. Criar perguntas para debate

Anote as dúvidas que surjam durante o desenvolvimento de sua história. Essas dúvidas podem levar a questionamentos entre os participantes do cenário.

12. Revise a sua história

Avalie o seu cenário várias vezes antes de apresentá-lo aos participantes. Pode ser difícil determinar quanto tempo levará para que os participantes concluam a história. Quando estiver em dúvida sobre a quantidade de tempo necessária, use de cautela. Se você notar que a sua apresentação está tomando muito tempo dos participantes, faça uma reavaliação.

13. Defina o tom do seu exercício

Quando os participantes chegarem para o exercício, estimule a participação de todos, qualquer que seja o seu nível na empresa ou tempo de serviço. O exercício dá a cada participante a oportunidade de compartilhar sua opinião e ajudar a organização a melhorar sua postura de segurança. Quanto mais os participantes se comunicarem e colaborarem entre si, maior será o valor que o exercício trará a todos.

14. Seja o moderador do exercício

A função do moderador é importante para manter a fluidez do exercício. Contudo, o moderador deve resistir à inclinação de participar. Nessa função, você estipula o cenário para os participantes e os ajuda a avançar. Você pode dar aos participantes tempo para debaterem diferentes tópicos da história e compartilharem perguntas e dúvidas para esclarecimento.

15. Rastreie os problemas

Certifique-se de que haja alguém para anotar os problemas e considerações que surjam durante o exercício. Você pode obter insights sobre questões que, do contrário, poderiam interferir na eficiência da sua história.

16. Siga a programação

Defina a duração do exercício e atenha-se a ela. Mantenha os participantes no percurso e relembre-os de continuar trabalhando na história conforme ela avança.

17. Avalie os seus resultados

Após seu exercício tabletop, analise os resultados e como podem ser integrados às operações diárias da sua organização. Por exemplo, se você realizou o teste com base em obrigações de conformidade, poderá criar um PDF que contenha as informações que os auditores necessitam.

Você também pode dar aos participantes a oportunidade de examinar as suas descobertas e executar o mesmo exercício em data posterior. Como isso, você poderá confirmar se as correções ou alterações ajudaram a lidar com os problemas que foram descobertos durante o exercício inicial.

Projeções e exercícios de exemplo de ransomware

Temos o prazer de compartilhar uma história tabletop de ransomware que desenvolvemos e executamos na Sophos: Ransomware Tabletop.

Você pode utilizá-la diretamente como está ou como base para desenvolver as suas próprias histórias.

Recursos tabletop de segurança cibernética

A CISA (Cybersecurity and Infrastructure Security Agency) dos EUA oferece recursos para ajudar as organizações na condução de seus próprios exercícios tabletop. Você pode acessar mais de 100 Exercícios Tabletop da CISA (CTEPs) designados para tratar de uma variedade de cenários de ameaça, incluindo:

- ✓ Segurança virtual: consiste em ransomware, ameaças internas, phishing, comprometimento de sistema de controle industrial (ICS) e outros cenários de segurança cibernética.
- ✓ Segurança física: inclui tiroteios, colisão de veículos, dispositivos explosivos improvisados, sistemas de aeronaves não tripuladas e outros cenários de segurança física.
- ✓ Convergência cibernética-física: foca na parte física dos vetores de ameaças e nos impactos cibernéticos dos vetores de ameaças físicas.

Além desses, a CISA oferece modelos pré-formulados que você pode usar para desenvolver os seus próprios exercícios tabletop.

Conclusão

A eficiência comprovada dos exercícios tabletop demonstra o seu papel crítico no preparo para a segurança cibernética moderna. As ameaças cibernéticas são cada vez mais proeminentes na era digital, forçando as organizações a adotarem e adaptarem esses exercícios para proteger suas operações. Ao entender os princípios básicos dos exercícios tabletop de segurança e implementar as práticas recomendadas neste documento, as organizações podem aprimorar sua resiliência contra ataques cibernéticos, assegurando que estejam bem preparadas para enfrentá-los e vencê-los.

Sophos Trust Center - https://www.sophos.com/pt-br/trust

Tabletop de Ransomware Sophos - https://assets.sophos.com/X24WTUEQ/at/hvsj54g5zq5hhcfb3xrfnmk/sophos-ransomware-tabletop-exercise-overview.pdf

Exercícios Tabletop CISA -https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

A transparência está no centro da filosofia da Sophos. Explore nosso Trust Center para ver mais informações e recursos.: www.sophos.com/trust

2024-07-24 (WP-DD)

SOPHOS