Folheto de soluções

SOPHOS

SERVIÇOS SOPHOS ADVISORY

Penetration Testing — Pentest

Validando as defesas de segurança através da simulação de métodos de ataque reais

Identificar vulnerabilidades e validar defesas de segurança com estratégias adaptadas e expertise independente, para aprimorar sua postura de segurança, reduzir riscos, facilitar a conformidade e melhorar sua eficiência operacional.

Reforça suas defesas e a postura de segurança proativamente

O acesso não autorizado a recursos da empresa, a exploração de vulnerabilidades novas e existentes, o uso de configurações incorretas e o abuso das políticas de segurança são sérios problemas de segurança. Verificar que aplicativos, redes e sistemas não estejam vulneráveis a riscos de segurança é essencial para tratar essas vulnerabilidades antes que possam ser exploradas pelos adversários. As varreduras e avaliações de vulnerabilidades são uma versão "light touch" para identificar lacunas e vulnerabilidades na sua rede, aprofundar os testes e validações necessários para demonstrar como um hacker obteria acesso ao seu ambiente e usaria todos esses sistemas como base para ataques mais profundos à sua rede.

Serviços do Sophos Penetration Testing

Pentests, ou testes de penetração ou intrusão, identificam e demonstram as vulnerabilidades da segurança cibernética, respondendo à pergunta: "Existe a possibilidade de um invasor conseguir entrar na minha rede?" O trabalho se desenvolve sob o prisma de ataques cibernéticos reais que são simulados para identificar vulnerabilidades em sistemas, redes e aplicativos. Os hackers éticos mais experientes exploram os possíveis pontos fracos e demonstram onde um invasor poderia chegar.

Há dois tipos primários de Pentest:

- **Pentest externo:** com foco em sistemas que são acessíveis pela Internet, como websites, VPNs e serviços voltados ao público. Simula um adversário tentando violar o seu perímetro de fora para dentro.
- **Pentest interno:** simula uma ameaça interna ou um invasor que já está dento do seu perímetro e avançando para sistemas, aplicativos e dados na rede interna.

A Sophos conduz cada pentest como deve ser: um teste único para uma organização única. Nossa metodologia baseada em metas é aplicada por profissionais de máxima segurança na indústria de testes, por meio de nossas táticas e inteligência de ameaça proprietárias fornecidas pelo grupo de inteligência de ameaça do Sophos X-Ops, e que inclui o Counter Threat Unit (CTU) — renomado por sua inteligência de informações e pesquisas em Advanced Persistent Threats (APT) e ataques patrocinados pelo Estado.

Benefícios

- Mais confiabilidade com os testes de controles de segurança internos e externos, incluindo proteções a recursos e sistemas de alto valor.
- Satisfaz metas de teste específicas através de modelos de ameaças e contexto que correspondem a um ambiente único.
- Receba uma sequência de ações para aplicar na correção.
- Conformidade regulatória, incluindo PCI DSS, HIPAA, GDPR, NIS, ISO 27001, SOC 2.
- Insights extraídos de informações recentes lançadas pelo grupo de inteligência de ameaça Sophos X-Ops.
- Determine o seu risco real de comprometimento.

Simule ataques avançados para testar suas defesas

As organizações devem conduzir pentests periodicamente não apenas para cumprir as regulamentações da indústria, mas para gerenciar proativamente a segurança cibernética em um cenário de ameaças complexo e avançado. Realizar pentests a intervalos regulares leva as organizações um passo à frente dos invasores, que continuamente adaptam suas técnicas e perícia para explorar novas vulnerabilidades. Os testes periódicos também ajudam a identificar pontos fracos criados devido a alterações feitas em infraestrutura, aplicativos ou integrações de terceiros. Além disso, um pentest proporciona dados realistas às organizações para entender sua exposição de risco, estratégias de remediação acionáveis e uma forma mensurável de rastrear as melhorias em segurança no decorrer do tempo.

Os benefícios do pentest incluem:

- **Redução proativa de risco:** as organizações que realizam testes regularmente enfrentam 50% menos incidentes de segurança, com 30% de redução em despesas gerais necessárias para gerenciar os incidentes de segurança.[1]
- **Cumprimento às conformidade:** normas e padrões regulamentares, como PCI DSS, HIPAA e ISO 27001, geralmente exigem pentests. Em fato, 73% das organizações mencionaram a conformidade como um motivador para o pentest.[2]
- **Economia em custos:** o custo médio de uma violação de dados é US$ 4,45 milhões[3], mas muitas vulnerabilidades podem ser tratadas por uma fração do custo usando os pentests.
- **Confiabilidade do cliente:** 65% dos consumidores dizem estar mais propensos a confiar em uma empresa que demonstra fortes práticas de segurança cibernética.[4]

Testar o seu pessoal

A inteligência artificial aumentou drasticamente a aposta em ataques de phishing, criando mensagens altamente sofisticadas e convincentes que são cada vez mais difíceis de detectar. Diferentemente dos tradicionais e-mails de phishing, com charadas, palavras enigmáticas, erros gramaticais e conteúdo genérico, um phishing realizado por IA pode gerar mensagens personalizadas com relevância contextual adaptada a indivíduos e organizações específicas. O resultado são os novos desafios que as equipes de segurança e os usuários terão para identificar e defender-se contra ataques de phishing, enfatizando a necessidade de treinamento continuado.

O nosso programa de pentest, Penetration Testing, pode ser combinado com ataques de phishing simulados para examinar a habilidade de seus funcionários em ponderar e responder às tentativas de phishing.

Recursos do serviço

- Regras de engajamento adaptadas, incluindo revisão dos sistemas de destino para dados críticos de negócios.
- Relatórios finais contendo descobertas detalhadas e sumário executivo.
- Opções para teste local e remoto.
- Opção de selecionar External Penetration Testing, Internal Penetration Testing e Phishing Attack Simulation Training para criar um cenário de ameaça combinado com um caso de uso especificamente voltado a você.
- Processo manual de teste conduzido por um profissional que inclui as táticas usadas pelos agentes de ameaças.
- Metodologia com base em metas que garante que os sistemas sejam testados em contextos mais amplos em seus ambientes.

O que está incluído no seu relatório

Sumário executivo: direcionado às pessoas não técnicas envolvidas no processo, de gerência sênior, auditores, conselho diretor e outros participantes importantes.

Descobertas detalhadas: escritas para o pessoal técnico para fornecer achados mais aprofundados e recomendações.

Metodologia de engajamento: define o escopo do engajamento e quais as atividades de teste realizadas.

Narrativa: descreve a sequência de ações adotadas pelo pessoal de teste para atingir as metas do engajamento, para auxiliar no entendimento de ameaças combinadas e/ou fases dependentes.

Recomendações: descobertas detalhadas, links para leituras avançadas e recomendações para corrigir ou reduzir o risco. O pessoal de teste reúne evidências de seus achados e, quando aplicável, e se possível, informação suficiente para replicar os achados usando ferramentas publicamente disponíveis.

Resultados do phishing (se aplicável): detalhes dos ataques de phishing utilizados e sua taxa de sucesso.

Outros serviços de teste da segurança cibernética

Não há avaliação independente ou técnica autônoma que ofereça melhor retrato da postura de segurança da organização. Cada teste adversário tem seus próprios objetivos e níveis de risco aceitáveis. A Sophos trabalha com você para determinar qual combinação de avaliações e técnicas deve ser usada para avaliar a sua postura de segurança e controles para identificar suas vulnerabilidades.

Saiba mais:
sophos.com/advisory-services

[1]Ponemon Institute [2]SANS Institute [3]IBM [4]PwC

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

© Copyright 2025. Sophos Ltd. Todos os direitos reservados.
Empresa registrada na Inglaterra e País de Gales sob o n°. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido
Sophos é marca registrada da Sophos Ltd. Todos os outros nomes de produtos e empresas mencionados são marcas comerciais ou marcas registradas de seus respectivos proprietários.

2025-06-05 BRPTBR (MP)

SOPHOS