Folheto de soluções

SOPHOS

Serviços Sophos Advisory

Redução de risco e resiliência proativas
frente ao avanço das ameaças cibernéticas

Avaliações de segurança personalizadas realizadas por especialistas

Diante da constante demanda da transformação digital, da ascensão da IA e das ameaças cibernéticas em evolução contínua, as organizações com visão de futuro reconhecem que a segurança cibernética é muito mais do que um desafio técnico: trata-se de uma prioridade estratégica. Os adversários com recursos avançados, o escrutínio regulatório e as expectativas das partes interessadas exigem uma abordagem proativa e abrangente à proteção de ativos digitais. O Serviços Sophos Advisory oferece conhecimento independente, experiência e estratégias personalizadas para identificar vulnerabilidades sistêmicas, reforçar as defesas e aprimorar a resiliência corporativa.

Por meio de táticas, técnicas e procedimentos (TTPs) do mundo real utilizadas pelos agentes de ameaças, nossos especialistas de segurança altamente certificados colocam à prova suas redes, sistemas e funcionários para ajudar sua empresa a:

- Identificar vulnerabilidades antes que sejam exploradas por invasores.
- Reforçar as defesas contra ameaças sofisticadas.
- Cumprir os requisitos regulamentares de conformidade.
- Avaliar a prontidão para resposta a incidentes.

- Construir uma relação de confiança com clientes, parceiros e partes interessadas

Reforço proativo da postura de segurança e defesa

Testes de penetração (pentest)

Os testes de penetração simulam ataques cibernéticos reais para identificar vulnerabilidades em sistemas, redes e aplicativos. Analistas experientes (hackers éticos) tentam explorar pontos fracos para demonstrar o que um invasor conseguiria fazer.

Há dois tipos principais de testes de penetração. Os testes de penetração externa se concentram em sistemas acessíveis pela internet, como sites, VPNs e serviços voltados ao público. Eles simulam um invasor externo tentando violar seu perímetro. Os testes de penetração interna simulam um agente ou invasor interno que já tenha conseguido violar o perímetro, e se concentram nos sistemas, aplicativos e dados da rede interna.

Isso é importante porque:

- Identifica vulnerabilidades ocultas que não são captadas por verificações de rotina.
- Oferece recomendações práticas para reforçar as defesas.
- Auxilia na conformidade regulatória (por exemplo, PCI DSS, HIPAA, GDPR, NIS, ISO 27001, SOC 2).
- Demonstra comprometimento com o gerenciamento proativo de riscos.
- Oferece cobertura abrangente contra riscos internos e no perímetro.

Principais perguntas respondidas pela solução:

- Onde estão as vulnerabilidades mais críticas em nossa infraestrutura?
- Com que facilidade um invasor poderia violar nossas defesas externamente?
- Caso um invasor obtenha acesso, quais riscos estão presentes internamente em nossa rede?
- Qual é o impacto potencial de um ataque bem-sucedido?
- Quais medidas podemos adotar para corrigir os pontos fracos identificados?

Testes de penetração da rede sem fio

Os testes de penetração da rede sem fio avaliam a segurança da infraestrutura e das redes Wi-Fi de uma organização e analisam sua conformidade com as regulamentações apropriadas. Os testes tentam explorar pontos fracos na criptografia, autenticação e controles de acesso.

Há dois escopos nos testes de penetração de rede sem fio. A avaliação passiva envolve o monitoramento do tráfego sem fio para identificar dispositivos não autorizados, pontos de acesso ilegítimos e configurações incorretas sem tentar conectar de forma ativa. A avaliação ativa simula um invasor tentando explorar vulnerabilidades na rede sem fio ao tentar decifrar a criptografia, contornar a autenticação e obter acesso não autorizado.

Isso é importante porque:

- Protege dados confidenciais transmitidos pelas redes sem fio.
- Identifica pontos de acesso ilegítimos e configurações incorretas.
- Garante que as políticas de segurança de rede sem fio estejam de acordo com as práticas recomendadas.
- Reduz o risco de violações de dados devido a vulnerabilidades na rede Wi-Fi.
- Avalia os riscos das exposições passiva e ativa.

Principais perguntas respondidas pela solução:

- Usuários não autorizados conseguem acessar nossas redes sem fio?
- Estamos usando criptografia forte e métodos seguros de autenticação?
- Há dispositivos ilegítimos conectados à nossa rede?
- Um invasor conseguiria contornar as proteções de nossa rede sem fio?
- Que medidas podemos tomar para melhorar a segurança da rede sem fio?

Avaliações de segurança de aplicativos Web

Geralmente, os aplicativos Web lidam com dados críticos da empresa e dos clientes, o que os torna alvos desejados pelos invasores. As avaliações de segurança de aplicativos Web oferecem a certeza de que seus aplicativos da Web estão protegidos ao se concentrarem em vulnerabilidades comuns, que incluem injeção de SQL, ataques de script entre sites (XSS) e falha na autenticação.

Tais avaliações podem envolver testes de caixa preta, em que o teste simula um invasor externo sem conhecimento anterior da mecânica interna do aplicativo ou dos testes de caixa branca. Nesse cenário, o analista tem acesso total ao código-fonte e à arquitetura, permitindo uma análise mais profunda das possíveis vulnerabilidades.

Isso é importante porque:

- Protege os dados, tanto da empresa como dos clientes, que são processados pelos aplicativos Web.
- Identifica falhas de configuração e de codificação que aumentam o risco.
- Apoiam a conformidade com padrões como OWASP Top 10 e PCI DSS.
- Reduz o risco de desfiguração de site, violações de dados e dano reputacional.
- Oferece tanto uma perspectiva externa como uma análise aprofundada da segurança dos aplicativos.

Principais perguntas respondidas pela solução:

- Nossos aplicativos Web estão vulneráveis a métodos comuns de ataque?
- Os dados confidenciais estão expostos em decorrência de falhas de codificação ou configurações incorretas?
- externo pode explorar vulnerabilidades, ou existem problemas mais profundos no código?
- Como podemos proteger autenticação de usuários e o gerenciamento de sessão?
- Quais medidas de remediação são necessárias para corrigir vulnerabilidades de aplicativos Web?

Resumo dos serviços de avaliação de segurança

Tipo de avaliação	Foco	Resposta a perguntas importantes	Cenários de exemplo
Testes de penetração (pentest)	Infraestrutura, sistemas e redes	Onde estão as vulnerabilidades? Como um invasor pode violar nossas defesas?	Externo: Testes de serviços e sites voltados ao público, Interno: Testes de controles de acesso interno e escalonamento de privilégio
Testes de penetração da rede sem fio	Segurança de Wi-Fi, criptografia e controles de acesso	Nosso Wi-Fi é seguro? Há dispositivos ilegítimos ou não autorizados?	Testes de segurança de Wi-Fi do escritório; Identificação de pontos de acesso ilegítimos; Tentativas de conexões não autorizadas
Avaliação de segurança de aplicativos Web	Aplicativos Web, falhas de codificação, autenticação	Nossos aplicativos são seguros? Há exposição de dados confidenciais? Como podemos corrigir vulnerabilidades?	Testes de portais do cliente, sites de e-commerce, aplicativos Web internos; Identificação de injeção de SQL, XSS ou falhas de autenticação

Outros serviços de testes de segurança cibernética

Nenhuma avaliação ou técnica individual e autônoma proporciona um panorama abrangente da segurança de uma organização. Cada teste adversarial tem seus próprios objetivos e níveis de risco aceitáveis. A Sophos pode trabalhar com você para determinar a combinação ideal de técnicas e avaliações para avaliar seus controles e postura de segurança a fim de identificar vulnerabilidades.

Saiba mais:
sophos.com/advisory-services

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

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

2025-05-30 BRPTBR (MP)