Folleto de la solución

SOPHOS

SERVICIOS DE ASESORAMIENTO DE SOPHOS

Pruebas de penetración

Valide las defensas de seguridad con métodos de ataque simulados reales

Identifique vulnerabilidades y valide las defensas de seguridad con conocimientos especializados independientes y estrategias personalizadas para mejorar su postura de seguridad, reducir el riesgo, facilitar el cumplimiento normativo y mejorar la eficiencia operativa.

Refuerce de forma proactiva las defensas y la postura de seguridad

Acceder sin autorización a los recursos de una empresa, explotar vulnerabilidades nuevas y existentes, aprovecharse de errores de configuración y sacar partido de políticas de seguridad deficientes son problemas de seguridad graves. Verificar que las aplicaciones, las redes y los sistemas no estén expuestos a riesgos de seguridad es fundamental para abordar estas vulnerabilidades antes de que las puedan aprovechar los atacantes. Si bien los escaneados y las evaluaciones de vulnerabilidades son una comprobación preliminar para identificar lagunas y vulnerabilidades en la red, se requieren pruebas y validaciones más exhaustivas para demostrar cómo un atacante podría obtener acceso al entorno y utilizar esos sistemas como base para lanzar ataques más profundos en la red.

Servicios de pruebas de penetración de Sophos

Las pruebas de penetración o pentests identifican y ponen de manifiesto vulnerabilidades de ciberseguridad, dando respuesta a la pregunta: "¿Podría un atacante infiltrarse en mi red?". Su funcionamiento consiste en simular ciberataques reales para identificar vulnerabilidades en sistemas, redes y aplicaciones. Los testers experimentados (hackers éticos) tratan de explotar las debilidades para demostrar cómo podría sacarles partido un atacante.

Existen dos tipos principales de pruebas de penetración:

- **Pruebas de penetración externas:** se centran en los sistemas a los que se puede acceder desde Internet, como sitios web, VPN y servicios de cara al público. Simulan un atacante que intenta vulnerar su perímetro desde el exterior.
- **Pruebas de penetración internas:** simulan una amenaza interna o un atacante que ya ha superado el perímetro, y se centran en los sistemas, las aplicaciones y los datos de la red interna.

Sophos aborda cada prueba de penetración de forma única para cada organización. La metodología basada en objetivos aplicada por los mejores testers de seguridad del sector utiliza nuestras informaciones y tácticas propias del grupo de información sobre amenazas Sophos X-Ops, que incluye la Counter Threat Unit (CTU), reconocida por sus conocimientos e investigación sobre amenazas avanzadas recurrentes (APT) y atacantes patrocinados por gobiernos.

Ventajas

- Obtenga garantías poniendo a prueba los controles de seguridad internos y externos, incluidas las protecciones de sistemas y recursos de gran valor.
- Cumpla los objetivos específicos de las pruebas mediante un modelo de amenazas y un contexto que se ajusten a su entorno único.
- Reciba medidas prácticas para la remediación.
- Respalde el cumplimiento normativo, como PCI DSS, HIPAA, RGPD, SRI, ISO 27001, SOC 2.
- Obtenga los datos más recientes del grupo de información sobre amenazas Sophos X-Ops.
- Determine su riesgo real de sufrir un ataque.

Simule ataques avanzados para poner a prueba sus defensas

Las organizaciones realizan pruebas de penetración periódicas no solo para cumplir con las normativas del sector, sino también para gestionar de forma proactiva el panorama cada vez más complejo y cambiante de las amenazas a la ciberseguridad. Al llevar a cabo pruebas de penetración a intervalos regulares, las organizaciones pueden adelantarse a los atacantes, que adaptan continuamente sus técnicas para explotar nuevas vulnerabilidades. Las pruebas periódicas también ayudan a identificar las debilidades introducidas por los cambios en la infraestructura, las aplicaciones o las integraciones de terceros. Además, las pruebas de penetración ofrecen a las organizaciones una visión realista de su exposición al riesgo, estrategias de remediación prácticas y una forma cuantificable de hacer un seguimiento de las mejoras de seguridad a lo largo del tiempo.

Entre las ventajas de las pruebas de penetración se incluyen:

- **Reducción proactiva de riesgos:** las organizaciones que realizan pruebas de penetración periódicas experimentan un 50 % menos de incidentes de seguridad y reducen en un 30 % el coste total de la gestión de incidentes de seguridad.[1]
- **Apoyo al cumplimiento normativo:** los marcos reguladores como PCI DSS, HIPAA e ISO 27001 suelen exigir pruebas de penetración. Según el 73 % de las organizaciones, el cumplimiento es uno de los factores que les impulsa a realizar pruebas de penetración.[2]
- **Ahorro de costes:** el coste medio de una filtración de datos es de 4,45 millones USD[3], pero muchas vulnerabilidades pueden subsanarse por una fracción de ese coste mediante pruebas de penetración.
- **Confianza de los clientes:** el 65 % de los clientes afirma que tiende a confiar más en una empresa que demuestra prácticas de ciberseguridad sólidas.[4]

Ponga a prueba a sus empleados

La inteligencia artificial ha aumentado drásticamente el riesgo de los ataques de phishing, ya que permite crear mensajes muy sofisticados y convincentes que son cada vez más difíciles de detectar. A diferencia de los correos de phishing tradicionales, plagados de errores gramaticales y contenido genérico, el phishing optimizado por IA puede generar mensajes personalizados y contextualmente relevantes, adaptados a personas u organizaciones específicas. Como resultado, tanto los equipos de seguridad como los usuarios se enfrentan a nuevos retos a la hora de identificar y defenderse de los ataques de phishing, lo que subraya la necesidad de formación continua.

Nuestro programa de pruebas de penetración se puede combinar con ataques simulados de phishing para evaluar la capacidad de sus empleados para detectar y responder a intentos de phishing.

Funciones del servicio

- Reglas personalizadas para la intervención, incluida la revisión de los sistemas objetivo que contienen datos críticos para la empresa.
- Informes finales con conclusiones detalladas y un resumen ejecutivo.
- Opciones de realización de pruebas in situ y a distancia.
- Opción de seleccionar pruebas de penetración externas, pruebas de penetración internas y formación y simulación de ataques de phishing para crear un escenario de amenazas mixto para su caso de uso específico.
- Proceso manual gestionado por los testers que incluye las tácticas utilizadas por los adversarios.
- Metodología basada en objetivos que garantiza que los sistemas se prueban en el contexto más amplio del entorno.

Qué se incluye en el informe

Resumen ejecutivo: dirigido a partes interesadas sin conocimientos técnicos, como altos cargos directivos, auditores, junta directiva y otras partes importantes.

Resultados detallados: redactados para el personal técnico a fin de proporcionar conclusiones y recomendaciones exhaustivas.

Metodología de la intervención: define el alcance de la intervención y las actividades de prueba que se han llevado a cabo.

Narrativa: describe la secuencia de acciones llevadas a cabo por los testers para alcanzar los objetivos de la intervención, con el fin de ayudar a comprender las amenazas mixtas y/o las fases dependientes.

Recomendaciones: detalla las averiguaciones, facilita el enlace a sitios web de lecturas adicionales y sugerencias para la remediación o la reducción de riesgos. Los testers aportan pruebas de sus observaciones cuando procede y, si es posible, información suficiente para replicar los resultados con herramientas disponibles públicamente.

Resultados de phishing (si procede): detalla los ataques de phishing utilizados y su índice de éxito.

Otros servicios de pruebas de seguridad

Ninguna evaluación o técnica individual aislada proporciona una visión completa de la postura de seguridad de una organización. Cada prueba de adversarios tiene sus propios objetivos y niveles de riesgo aceptables. Sophos puede trabajar con su organización para determinar la combinación de pruebas y técnicas que debe utilizar para evaluar su postura de seguridad y sus controles a fin de identificar sus vulnerabilidades.

Más información:
es.sophos.com/advisory-services

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

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2025-06-05 BRES (MP)

SOPHOS