Brochure

SOPHOS

SOPHOS ADVISORY SERVICES

Penetration Test

Metti alla prova i tuoi sistemi di difesa con simulazioni di attacco realistiche

Identifica le vulnerabilità e metti alla prova le tue difese di sicurezza con l'aiuto di esperti indipendenti che mettono al tuo servizio la loro esperienza e realizzano strategie personalizzate per migliorare il tuo profilo di sicurezza, ridurre il rischio, semplificare il rispetto della conformità e ottimizzare la tua efficienza operativa.

Potenzia proattivamente le tue difese e il tuo profilo di sicurezza

L'accesso non autorizzato alle risorse aziendali, l'exploit di vulnerabilità nuove o esistenti, nonché lo sfruttamento di errori di configurazione e policy di sicurezza mal formulate sono tutti problemi di sicurezza estremamente seri. Assicurarsi che applicazioni, reti e sistemi non siano vulnerabili ai rischi di sicurezza è fondamentale per rimediare a queste vulnerabilità prima che possano essere sfruttare dai cybercriminali. Mentre scansioni e valutazioni delle vulnerabilità sono analisi "più superficiali" per identificare eventuali lacune e vulnerabilità della rete, occorrono verifiche e test più dettagliati per dimostrare come un cybercriminale potrebbe accedere al tuo ambiente e utilizzare quei sistemi come base per sferrare attacchi in parti più profonde della rete.

Servizi di penetration testing Sophos

I penetration test, o "pen test", identificano e forniscono una dimostrazione delle vulnerabilità di cybersecurity, rispondendo alla domanda: "È possibile che un cybercriminale riesca a infiltrarsi nella mia rete?". Agiscono simulando attacchi informatici reali per identificare la presenza di vulnerabilità in sistemi, reti e applicazioni. Tester esperti (ethical hacker) cercano di sfruttare i punti deboli degli ambienti per dimostrare quali obiettivi potrebbe colpire un cybercriminale.

Esistono due principali tipi di penetration test:

- **Penetration test esterni:** si concentrano sui sistemi ai quali è possibile accedere da Internet, come siti web, VPN e servizi rivolti al pubblico. Simulano i tentativi di un cybercriminale di violare il tuo perimetro di rete dall'esterno.
- **Penetration test interni:** simulano una minaccia interna o un cybercriminale che si è già infiltrato nel perimetro di rete, concentrandosi su sistemi, applicazioni e dati situati nella rete interna.

Per i penetration test, Sophos adotta un approccio unico e personalizzato per ogni azienda. La nostra metodologia basata su obiettivi viene messa in atto dai migliori tester di sicurezza del settore, utilizzando le nostre tattiche esclusive e i dati di intelligence sulle minacce forniti dal gruppo Sophos X-Ops, che include la Counter Threat Unit (CTU), conosciuta per l'intelligence e le ricerche svolte su advanced persistent threat (APT) e hacker finanziati a livello statale.

Vantaggi

- Maggiore tranquillità, grazie ai test sui controlli interni ed esterni, incluse le soluzioni di protezione che tutelano risorse e sistemi critici.
- Raggiungimento di obiettivi di test specifici, attraverso l'uso di un modello per le minacce e di un contesto perfettamente adatti all'unicità del tuo ambiente.
- Indicazioni pratiche per le azioni di correzione.
- Supporto della conformità alle normative, incluse PCI DSS, HIPAA, GDPR, NIS, ISO 27001, SOC 2.
- Approfondimenti derivati dai più recenti dati di intelligence sulle minacce del gruppo Sophos X-Ops.
- Determinazione del rischio realistico di compromissione.

Simula attacchi avanzati per mettere alla prova le tue difese

Le aziende che conducono penetration test a cadenza regolare non rispettano solo la conformità alle normative di settore, ma gestiscono anche proattivamente le proprie difese in un panorama delle minacce informatiche sempre più complesso e mutevole. Svolgendo ciclicamente penetration test, le aziende possono rimanere al passo con i cybercriminali che adattano continuamente le proprie tecniche per sfruttare nuove vulnerabilità. L'esecuzione regolare di test aiuta anche a identificare le vulnerabilità introdotte attraverso cambiamenti nelle infrastrutture, nelle applicazioni o nelle integrazioni di terze parti. Inoltre, i penetration test offrono alle imprese un quadro realistico della loro esposizione al rischio, proponendo anche strategie di correzione pratiche e un sistema misurabile per monitorare i miglioramenti della propria sicurezza nel tempo.

I vantaggi dei penetration test includono:

- **Riduzione proattiva del rischio:** le aziende che conducono regolarmente penetration test subiscono il 50% di incidenti in meno e usufruiscono di una riduzione del 30% dei costi complessivi di gestione degli incidenti di sicurezza[1].
- **Supporto per la conformità:** spesso quadri normativi come PCI DSS, HIPAA e ISO 27001 prescrivono penetration test. Il 73% delle aziende dichiara infatti che la conformità è uno dei motivi per cui conducono penetration test[2].
- **Risparmi sui costi:** il costo medio di una violazione dei dati è pari a 4,45 milioni di $[3], ma con i penetration test molte vulnerabilità possono essere risolte con una spesa inferiore rispetto a questa cifra.
- **Fiducia dei clienti:** il 65% dei consumatori sostiene che la probabilità che ripongano fiducia in un'azienda è maggiore quando quest'ultima dimostra di adottare pratiche di cybersecurity efficaci[4].

Metti alla prova il tuo team

L'intelligenza artificiale ha aumentato drasticamente la posta in gioco per gli attacchi di phishing, creando messaggi sofisticati e convincenti che sono sempre più difficili da riconoscere come fasulli. A differenza delle tradizionali e-mail di phishing, tempestate di errori grammaticali e contenuti generici, il phishing basato sull'IA è in grado di generare messaggi personalizzati e contestualmente pertinenti, personalizzati per essere inviati a persone oppure organizzazioni specifiche. Di conseguenza, sia i team di sicurezza che gli utenti si trovano ad affrontare nuove sfide nell'identificare e proteggere i sistemi dagli attacchi di phishing, il che dimostra l'esigenza di formazione continua.

Il nostro programma di penetration testing può essere utilizzato in combinazione con simulazioni di attacchi di phishing per valutare la capacità dei tuoi dipendenti di riconoscere e rispondere ai tentativi di phishing.

Caratteristiche del servizio

- Regole di incarico personalizzate, inclusa una revisione dei sistemi testati, tenendo conto dei dati business-critical.
- Report finali con risultati dettagliati e un riepilogo non tecnico.
- Opzioni di test on-premise e da remoto.
- La possibilità di scegliere tra penetration test esterni, penetration test interni e formazione con simulazioni di attacchi di phishing, per creare uno scenario con minacce combinate che rifletta le tue esigenze specifiche.
- Processo manuale e diretto dal tester, che include le stesse tattiche sfruttate dai cybercriminali.
- Metodologia basata sugli obiettivi, che garantisce che i sistemi vengano testati nel contesto più ampio dell'intero ambiente.

Cosa include il tuo report

Riepilogo non tecnico: rivolto a stakeholder senza competenze tecniche specializzate, ovvero Senior Management, auditor, consigli di amministrazione e altre parti importanti.

Risultati dettagliati: scritti per fornire al personale tecnico dettagli approfonditi sui risultati e raccomandazioni.

Metodologia dell'incarico: definisce l'ambito di applicazione dell'incarico e indica i test che sono stati svolti.

Narrazione: descrive la sequenza di azioni intraprese dai tester per raggiungere gli obiettivi dell'incarico, per aiutare a comprendere le minacce combinate e/o le fasi dipendenti.

Raccomandazioni: forniscono tutti i dettagli dei risultati, con link a pagine web per letture di approfondimento, nonché raccomandazioni per la correzione o la riduzione dei rischi. I tester forniscono prova dei risultati ottenuti (se applicabile) e, se possibile, indicano le informazioni necessarie per replicare i risultati con strumenti disponibili pubblicamente.

Risultati delle simulazioni di phishing (se applicabili): dettagli sugli attacchi di phishing utilizzati e sul loro tasso di successo.

Altri servizi di test della cybersecurity

Nessuna singola valutazione o tecnica individuale offre un quadro completo del profilo di sicurezza di un'azienda. Ogni test di simulazione di attacco ha obiettivi e livelli accettabili di rischio diversi. Sophos può collaborare con te per aiutarti a definire la combinazione di valutazioni e tecniche più adatta per esaminare il tuo profilo e i tuoi controlli di sicurezza specifici, al fine di identificare le vulnerabilità dei tuoi sistemi.

Scopri di più:
sophos.it/advisory-services

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

Vendite per Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

2025-06-05 BRIT (MP)

SOPHOS