Sophos Advisory Services

Riduzione proattiva dei rischi e resilienza di fronte a cyberminacce sempre più evolute

Valutazioni di sicurezza personalizzate e svolte da esperti

Con le continue esigenze della trasformazione digitale, l'ascesa dell'IA e la presenza di minacce informatiche in continua evoluzione, le organizzazioni più lungimiranti riconoscono che la cybersecurity non è solo una sfida tecnica, bensì una priorità strategica. Active adversary sempre più avanzati, controlli normativi e stakeholder con aspettative elevate sono tutti fattori che richiedono un approccio proattivo e completo alla protezione delle risorse digitali. I Sophos Advisory Services mettono a tua disposizione l'esperienza, le competenze indipendenti e le strategie personalizzate necessarie per identificare vulnerabilità sistemiche, potenziare le difese e incrementare la resilienza dell'azienda.

Basandosi sulle stesse tattiche, tecniche e procedure (TTP) sfruttate dai cybercriminali, i nostri esperti di sicurezza altamente qualificati mettono alla prova reti, sistemi e dipendenti, per aiutare la tua organizzazione a:

- Identificare le vulnerabilità prima che i cybercriminali possano sfruttarle.
- Potenziare i sistemi di difesa contro le minacce più sofisticate.
- Soddisfare i requisiti di conformità normativa.
- Valutare la preparazione all'incident response.
- Stabilire un rapporto di fiducia con clienti, partner e stakeholder.

Potenzia proattivamente le tue difese e il tuo profilo di sicurezza

Penetration test (pen test)

I penetration test simulano 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. I 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 hacker di violare il tuo perimetro di rete dall'esterno. I penetration test interni simulano invece 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.

Perché sono importanti:

- Identificano vulnerabilità nascoste che potrebbero sfuggire durante le scansioni di routine.
- Offrono raccomandazioni pratiche per potenziare i sistemi di difesa.
- Supportano la conformità alle normative (ad es. PCI DSS, HIPAA, GDPR, NIS, ISO 27001, SOC 2).
- Dimostrano il tuo impegno verso una gestione proattiva del rischio.
- Svolgono indagini complete sui rischi di sicurezza sia a livello di perimetro di rete, che interno.

Le principali domande a cui offre risposta:

- Dove si trovano le vulnerabilità più critiche nella nostra infrastruttura?
- Con quanta facilità riuscirebbe un hacker a fare breccia nelle nostre difese dall'esterno?
- Quali sarebbero i rischi all'interno della rete, se un cybercriminale riuscisse a ottenere l'accesso?
- Qual è il potenziale impatto di un attacco andato a segno?
- Quali misure possiamo adottare per eliminare i punti deboli identificati?

Test di penetration per le reti wireless

I test di penetration per le reti wireless valutano la protezione delle reti Wi-Fi e dell'infrastruttura di un'organizzazione, esaminandone la conformità ai mandati applicabili. I tester cercano di sfruttare i punti deboli nella crittografia, nell'autenticazione e nei controlli di accesso.

I test di penetration per il wireless prevedono due ambiti di applicazione. La valutazione passiva monitora il traffico wireless per identificare dispositivi non approvati, access point non autorizzati ed errori di configurazione, senza alcun tentativo attivo di connessione. La valutazione attiva simula le azioni di un hacker che cerca di sfruttare vulnerabilità nella rete wireless per decrittografare gli elementi crittografati, eludere l'autenticazione e ottenere accesso non autorizzato.

Perché sono importanti:

- Aiutano a proteggere i dati di natura sensibile trasmessi sulle reti wireless.
- Identificano gli access point non autorizzati e gli errori di configurazione.
- Garantiscono l'allineamento delle policy di sicurezza per il wireless con le best practice applicabili.
- Riducono il rischio di violazioni dei dati causate da vulnerabilità della rete Wi-Fi.
- Valutano sia il rischio di esposizione passiva, che quello di exploit attivo.

Le principali domande a cui offre risposta:

- È possibile che gli utenti non autorizzati accedano alla nostra rete wireless?
- Utilizziamo un sistema di crittografia efficace e metodi di autenticazione sicuri?
- Ci sono dispositivi non autorizzati connessi alla nostra rete?
- Può un hacker eludere i nostri sistemi di protezione della rete wireless?
- Quali misure possiamo adottare per migliorare la sicurezza della rete wireless?

Valutazioni della sicurezza delle applicazioni web

Spesso le applicazioni web gestiscono dati commerciali e dei clienti di natura critica, e questo le rende uno dei principali bersagli dei cybercriminali. Le valutazioni della sicurezza delle applicazioni web offrono la certezza che le tue applicazioni web sono protette, in quanto si concentrano sull'individuazione delle vulnerabilità più comuni, inclusi gli attacchi di SQL injection e cross-site scripting (XSS), e di sistemi di autenticazione difettosi.

Queste valutazioni possono includere test "black box" (nel corso dei quali il tester simula l'attività di un hacker esterno senza alcuna conoscenza dei meccanismi interni dell'applicazione) o test "white box" (nei quali il tester ha accesso completo al codice sorgente e all'architettura dell'applicazione, per permettere un'analisi più approfondita delle potenziali vulnerabilità).

Perché sono importanti:

- Proteggono i dati dei clienti e dell'azienda che vengono gestiti dalle applicazioni web.
- Identificano i difetti del codice e gli errori di configurazione che aumentano il livello di rischio.
- Supportano la conformità a standard come OWASP Top 10 e PCI DSS.
- Riducono il rischio di deturpazione dei siti web, violazioni dei dati e danni alla reputazione.
- Offrono sia una prospettiva esterna, che un'analisi interna approfondita della sicurezza di un'applicazione.

Le principali domande a cui offre risposta:

- Le nostre applicazioni web sono vulnerabili ai più comuni metodi di attacco?
- Sono presenti difetti del codice o errori di configurazione che espongono i dati di natura sensibile a rischi?
- Ci sono vulnerabilità che un hacker esterno è in grado di sfruttare? O sono presenti problemi maggiormente radicati nel codice?
- Come possiamo proteggere l'autenticazione degli utenti e la gestione delle sessioni?
- Quali misure di correzione sono richieste per eliminare le vulnerabilità delle applicazioni web?

Riepilogo dei servizi di valutazione della sicurezza

Tipo di valutazione	Ambito specifico	Principali domande a cui offre risposta	Scenari di esempio
Penetration test (pen test)	Infrastruttura, sistemi e reti	Dove sono le vulnerabilità? Come può un hacker a fare breccia nelle nostre difese?	Esterno: test di siti web e servizi rivolti al pubblico; interno: test di controlli di accesso e privilege escalation interni
Test di penetration per le reti wireless	Sicurezza del Wi-Fi, crittografia, controlli di accesso	La nostra rete Wi-Fi è sicura? Ci sono dispositivi non autorizzati o non approvati?	Test della sicurezza del Wi-Fi dell'ufficio; identificazione degli access point non autorizzati; tentativi di stabilire connessioni non autorizzate
Valutazione della sicurezza delle applicazioni web	Applicazioni web, difetti del codice, autenticazione	Le nostre app sono protette? Ci sono dati sensibili esposti a rischi? Come possiamo risolvere le vulnerabilità?	Test sui portali dei clienti, sui siti di e-commerce, sulle app web interne; identificazione di SQL injection, XSS o sistemi di autenticazione difettosi

Altri servizi che offrono test di cybersecurity

Nessuna singola valutazione o tecnica individuale offre un quadro completo della sicurezza di un'organizzazione. 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 alle tue esigenze, per valutare il tuo profilo e i tuoi controlli di sicurezza, al fine di identificare le tue vulnerabilità.

Scopri di più:
sophos.it/advisory-services

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