



Sempre di piu' al centro del mirino

Sempre piu' spesso i siti web e le applicazioni online stanno diventando gli obiettivi privilegiati di attacchi informatici che, a vario titolo, sfruttano le vulnerabilita' presenti all'interno delle applicazioni e dei sistemi su cui tali applicazioni sono installate per orchestrare attacchi basati su tecniche sempre piu' evolute e sempre piu' difficili da rilevare. Dai tradizionali attacchi di "defacement" del sito web, agli attacchi basati su SQL Injection indirizzati a sottrarre le informazioni memorizzate all'interno delle applicazioni o ad iniettare malware e codice malevolo all'interno delle pagine del sito web fino alle tecniche di Cross Site Scripting (XSS) indirizzate a sfruttare i privilegi degli utenti autorizzati dell'applicazioni per eseguire attivita' illecite, il fenomeno degli attacchi a siti web e applicazioni online e' sempre piu' diffuso e sempre piu' portato alla ribalta della cronaca.

Parallelamente, se nell'ambito della gestione delle problematiche di sicurezza nell'ambito di sistemi e apparati di rete e' in tempi recenti migliorata la sensibilita' degli amministratori di sistema rispetto alle problematiche correlate al "patching" e alla gestione dei criteri di sicurezza, nell'ambito dello sviluppo applicativo resta ancora molto da fare in termini di sensibilizzazione degli sviluppatori rispetto alle linee guida da rispettare nell'ottica di garantire elevati standard di sicurezza nell'ambito delle proprie attivita' di sviluppo. Questo contesto rappresenta pero' un terreno fertile per le comunita' Cyber Criminali che sempre piu' spesso trovano nei siti web e nelle applicazioni online quei "punti deboli" attraverso cui perpetrare le proprie attivita' illecite. In aggiunta a quanto sopra, gli elevati livelli di complessita' e di costo delle soluzioni oggi disponibili per la protezione dei siti web e delle applicazioni online, abbinato ad uno scenario che sempre piu' spesso vede le aziende utilizzare un numero sempre piu' ampio di fornitori di servizi di sviluppo applicativo e di hosting - non ultimo a seguito della diffusione dei servizi basati su cloud - rende difficile e costosa, in particolare per aziende di dimensioni piccole e medie, l'adozione di strumenti che consentano di adeguare le proprie procedure di sicurezza all'attuale livello delle minacce.

Analisi di sicurezza "as a service" per siti web e applicazioni online
Effettua un'analisi di sicurezza delle applicazioni web dentro e fuori l'azienda
Rileva vulnerabilita' ad attacchi come SQL Injection e Cross Site Scripting (XSS)
Rileva vulnerabilita' ad attacchi di Distributed Denial of Service (DDoS) applicativo
Rileva vulnerabilita' nell'ambito dei protocolli e delle librerie SSL utilizzate
Rileva vulnerabilita' nell'ambito dei cookie e dei form di autenticazione
Supporta la conformita' a severi standard di come OWASP, ISO27001, PCI-DSS
Fornisce report di facile lettura ai manager, report dettagliati agli sviluppatori
Fornito "as a service" direttamente dal nostro Private Cloud
Nessun investimento richiesto in hardware e software

100%

#SECURITY

#CLOUD

#SAAS

Auditing "as a service" per siti web e applicazioni online

CloudWALL WAS | Web Application Security e' la soluzione "as a service", fornita direttamente dai Security Operation Center (SOC) di CloudWALL Italia, in grado di fornire un'analisi dettagliata delle problematiche di sicurezza e conformita' alle politiche di sicurezza dell'azienda, nonche' a stringenti standard internazionali come OWASP, ISO27001, PCI-DSS, nell'ambito dei siti web e delle applicazioni pubblicate dentro e fuori l'azienda.

Grazie ad un potente motore di analisi delle applicazioni web e degli oggetti che la costituiscono, CloudWALL WAS | Web Application Security non solo e' in grado di rilevare la presenza di vulnerabilita' nell'ambito dell'applicazione - comprese vulnerabilita' ad attacchi quali SQL Injection, Cross Site Scripting (XSS) e HTTP Slow Post (DDoS) - ma anche di individuare fattori di non conformita' alle normative di riferimento - prima fra tutte OWASP - relative a scelte di sviluppo non corrette in termini di sicurezza nell'ambito dei "cookie", dei protocolli di comunicazione utilizzati per transazioni sensibili - come ad esempio legate ad un processo di autenticazione (HTTP vs. HTTPS) della presenza di funzionalita' di "auto-complete" nell'ambito dei form di autenticazione degli utenti o ancora di una mancata gestione degli "errori" dell'applicazione che e' uno degli strumenti tipicamente utilizzati da un "attacker" nelle fasi di raccolta delle informazioni propedeutiche alla predisposizione di un attacco.

Tutte le informazioni rilevate nell'ambito dell'analisi sono consolidate in formati di reportistica differenziati in funzione dell'utente destinatario : agli sviluppatori e agli amministratori di sistema saranno forniti report dettagliati che illustrano in particolareggiato le vulnerabilita' rilevate, gli oggetti impattati, la severita' e le possibili modalita' di sfruttamento della vulnerabilita' nonche' le linee guida per porvi rimedio; ai manager di riferimento saranno invece forniti report di sintesi che consentano di comprendere a colpo d'occhio, grazie a grafici di semplice lettura e comprensione, gli esiti dei test effettuati ed il livello di severita' delle problematiche di sicurezza rilevate.

Fornito direttamente dal nostro Private Cloud

CloudWALL WAS | Web Application Security e' fornito in modalita' SaaS (Software as a Service) direttamente dal Private Cloud di CloudWALL Italia.

Grazie all'architettura centralizzata presso il nostro Private Cloud, CloudWALL WAS | Web Application Security viene fornito totalmente in modalita' "as a service" e non richiede l'acquisto, l'installazione e la gestione di piattaforme hardware e software, costose da acquisire e complesse da gestire, ma soltanto l'attivazione di un servizio che consente di analizzare direttamente dal nostro Private Cloud tutte le applicazioni esposte, indipendentemente se siano installate all'interno del proprio Data Center o presso terze parti.



Per l'analisi delle applicazioni pubblicate internamente alla rete locale aziendale, viene invece fornita una Virtual Appliance pronta per l'uso che puo' essere installata all'interno di qualsiasi infrastruttura di virtualizzazione basata su VMware o Microsoft Hyper-V.

Grazie alla granulare capacita' di analisi che consente di minimizzare i falsi positivi e ad un motore di reportistica avanzato in grado di guidare gli sviluppatori nel processo di revisione delle applicazioni, CloudWALL WAS | Web Application Security rappresenta la risposta ottimale per supportare l'introduzione di politiche e procedure per la sicurezza e la conformita' nell'ambito dei processi di Software Development Life Cycle (SDLC).

www.cloudwall.tk
info@cloudwall.tk

NO HARDWARE
SOFTWARE
MAINTENANCE

CLOUDWALL
SECURITY AS A SERVICE

Linee guida dettagliate per gli sviluppatori, dashboard sintetiche per il manager

CloudWALL WAS | Web Application Security e' stato progettato per mettere a disposizione di chi sviluppa siti e applicazioni web ma anche dei rispettivi finali che utilizzano tali applicazioni per gestire i propri contenuti e la propria reputazione aziendale gli strumenti necessari per verificare il livello di sicurezza dei propri siti web e delle proprie applicazioni online rispetto ai sempre piu' diffusi attacchi di livello di applicativo, tra cui Cross Site Scripting (XSS) e SQL Injection solo per citare i piu' noti.

Parallelamente, CloudWALL WAS | Web Application Security fornisce le indicazioni sulla conformita' dei siti web e delle applicazioni online rispetto alle "best practices" di riferimento nonche' rispetto a severe normative quali OWASP (Open Web Application Security Project), ISO27001 e PCI-DSS.

L'analisi di sicurezza ha lo scopo di valutare la sicurezza e la conformita' alle "best practices" delle applicazioni in ambiti quali :

- Validazione dei parametri forniti in input dall'utente
- Efficacia dei controlli di accesso, nella gestione degli account e delle sessioni applicative
- Vulnerabilita' a iniezione di comandi (SQL Injection) e Cross-Site scripting (XSS)
- Vulnerabilita' a Buffer Overflow, di amministrazione remota e della configurazione del server web
- Errata gestione degli errori applicativi e delle procedure di crittografia

A partire dalle informazioni collezionate, vengono consolidati i risultati ottenuti dai test effettuati con particolare riferimento alla severita' delle vulnerabilita' rilevate, alla ricorrenza e diffusione all'interno dei sistemi e dei servizi censiti, agli impatti delle varie vulnerabilita', alla complessita' delle tecniche di attacco per lo sfruttamento, alle "best practices" per la mitigazione delle vulnerabilita' rilevate.

Tali informazioni sono consolidate all'interno della reportistica analitica fornita agli sviluppatori e amministratori di sistema.

Parallelamente, a partire dai risultati viene generata un report di sintesi, destinato ai manager di riferimento, che attraverso grafici di semplice lettura fornisce una panoramica sintetica di quanto emerso nell'ambito dei test di sicurezza effettuati nell'ambito dei siti web e delle applicazioni online censite.

A supporto degli sviluppatori e degli amministratori di sistema interessati ad comprendere le attivita' necessarie per la risoluzione dei problemi di sicurezza rilevati, o dei manager interessati a quantificare il fattore di rischio rilevato sono a disposizione gli analisti del Security Operation Center di CloudWALL Italia.

Security Audit "as a service" direttamente dai nostri SOC

Analisi di sicurezza "as a service" per siti web e applicazioni online

Effettua un'analisi di sicurezza delle applicazioni web dentro e fuori l'azienda

Rileva vulnerabilita' ad attacchi come SQL Injection e Cross Site Scripting (XSS)

Rileva vulnerabilita' ad attacchi di Distributed Denial of Service (DDoS) applicativo

Rileva vulnerabilita' nell'ambito dei protocolli e delle librerie SSL utilizzate

Rileva vulnerabilita' nell'ambito dei cookie e dei form di autenticazione

Supporta la conformita' a severi standard di riferimento come OWASP, ISO27001, PCI-DSS

Fornisce report di facile lettura ai manager, report dettagliati agli sviluppatori

Fornito "as a service" direttamente dal nostro Private Cloud

Nessun investimento richiesto in hardware e software

Un ecosistema di soluzioni integrate

CloudWALL WAS | Web Application Security si integra con altre soluzioni "as a service" fornite dal Private Cloud di CloudWALL Italia :

- Con CloudWALL WAF | Web Application Firewall per fornire una protezione attiva per siti web e applicazioni online da attacchi applicativi quali SQL Injection e Cross Site Scripting (XSS) e garantire la conformita' a severi standard internazionali come OWASP, ISO27001, PCI-DSS;
- Con CloudWALL VAM | Vulnerability Management per rilevare la presenza di vulnerabilita' nell'ambito dei sistemi interni ed esterni all'azienda ed indirizzare un processo periodico di gestione delle vulnerabilita' che tenga conto della severita' delle vulnerabilita' ma anche del valore degli asset impattati;
- Con CloudWALL MON | Availability Monitoring, per garantire il monitoraggio della disponibilita' e dei livelli di servizio offerti dai siti web e dalle applicazioni online per gli utenti che vi accedono da qualsiasi parte nel mondo;

www.cloudwall.tk
info@cloudwall.tk


CLOUDWALL
SECURITY AS A SERVICE

CloudWALL Italia nasce su iniziativa di un team di professionisti con esperienze decennali nel mondo della Cyber Security che nel 2013 decidono di unire le proprie forze con lo scopo di supportare aziende e partner di canale nel cogliere le opportunità offerte dalle moderne tecnologie in Cloud per realizzare nuove soluzioni e nuovi servizi ad alto valore aggiunto per la sicurezza del sistema informativo aziendale.

Grazie all'esperienza maturata in anni di "scouting" di nuove tecnologie e ad una profonda conoscenza del mercato delle tecnologie e delle soluzioni disponibili sul mercato mondiale, siamo stati tra gli "early adopter" di molte delle tecnologie di IT Security basate su Cloud oggi disponibili sul mercato e partecipiamo tuttora ai programmi di "beta testing" in collaborazione con i provider internazionali di servizi "cloud-based".



La nostra offerta e' costituita da un ampio portafoglio di soluzioni per garantire la sicurezza del sistema informativo aziendale, l'integrita' e la confidenzialita' dei dati e dei contenuti, la protezione dell'identita' degli utenti. Tutte le nostre soluzioni sono caratterizzate da una architettura centralizzata nel nostro Private Cloud e da un approccio "as a service" che non richiede investimenti iniziali e che garantisce tempi di messa in opera estremamente ridotti.

Grazie a queste caratteristiche, la nostra offerta e' caratterizzata da :

- Architettura centralizzata presso il nostro Private Cloud
- Modalita' di approccio totalmente "as a service"
- Tempi di rilascio e messa in opera estremamente ridotti
- Nessun investimento in hardware e software
- Nessun onere sistemistico e di conduzione operativa
- Costi limitati rispetto a soluzioni "on premise"
- Supporto da parte dei Security Engineer di CloudWALL Italia

Attraverso un'offerta ampia e modulare di soluzioni per la sicurezza del sistema informativo, dei dati e dell'identita' degli utenti, ad una architettura centralizzata nel nostro Private Cloud e ad un approccio totalmente "as a service", CloudWALL Italia e' l'interlocutore ideale per partner di canale, system integrator e fornitori di servizi IT interessati a sfruttare le potenzialita' offerte dalle nostre tecnologie per proporre ai propri clienti nuove soluzioni valore aggiunto e nuovi servizi gestiti in modalita' di Managed Service Provider (MSP) senza la necessita' di prevedere quegli investimenti iniziali in hardware, software, connettivita' e competenze specialistiche tipicamente richiesti per la realizzazione di soluzioni con un approccio "on premise".

Distribuito da

