Digital Security

Cyber Security

Verifica il grado di vulnerabilità del tuo sistema informatico

Individua gli interventi idonei alla messa in sicurezza della proprietà informatica grazie ai nostri servizi di Cyber Security, una soluzione per ogni esigenza.

Vulnerability Assessment and Mitigation

Il metodo del Vulnerability Assessment and Mitigation (VAM), adottato dalla Divisione Cyber Security di INSIDE, si compone di una serie di attività non invasive volte a **valutare l'efficacia e il grado di robustezza dei sistemi di sicurezza** adottati dalla vostra azienda, individuandone le vulnerabilità note in caso di attacco informatico. A queste prime fasi d'intervento segue l'adozione di contromisure finalizzate al miglioramento della sicurezza dei vostri sistemi.

L'adozione del VAM deve essere organizzata periodicamente durante l'anno, in quanto la tecnologia è in continuo progresso e con essa anche gli strumenti per attaccare un sistema.

La Divisione Cyber Security di INSIDE sviluppa i seguenti livelli di VAM:

- **Data Base**: la nostra analisi si concentra in particolare sui DB maggiormante utilizzati dalle aziende (SQL Server Microsoft, Orcale, SyBase Server, etc.). L'intervento avviene attraverso l'uso di strumenti e software sofisticatissimi e prevede una scansione automatica di queste banche dati, allo scopo di individuare e analizzare i punti deboli e quindi più facili da attaccare. Ogni azienda "conserva" le informazioni aziendali all'interno di questi DataBase che, essendo costantemente riorganizzati per una loro migliore fruibilità, sono esposti ad attacchi di malintenzionati, quali aziende concorrenti.
- **Rete Telefonica**: l'attacco alla rete telefonica è comunemente chiamato WarDial. Si tratta di un attacco informatico utilizzato frequentemente, poiché la rete telefonica risulta maggiormente vulnerabile per la presenza dei cosiddetti bachi (bug). L'intervento si focalizza sulla scansione di tutta la rete telefonica composta da centralini, modem, apparecchiature telefoniche, etc.

Penetration Test

Valuta la sicurezza di una rete o di un sistema

Il Penetration Test è un servizio di valutazione della sicurezza di un sistema o di una rete, mediante la simulazione di un attacco da parte di un agente di minaccia esterno o interno. L'obiettivo è quello di evidenziare le debolezze della piattaforma, fornendo il maggior numero di informazioni sulle vulnerabilità tecnologiche che ne hanno permesso l'accesso non autorizzato: si tratta, sostanzialmente di vestire i "panni" di un vero hacker, il quale, sfruttando le vulnerabilità rilevate, è in grado di ottenere ogni informazione necessaria per l'accesso all'infrastruttura informatica.

Web Application Penetration Testing

Test di sicurezza informatica su applicazioni web

Con l'avvento dell'E-Commerce, le aziende sempre più spesso utilizzano il web per promuovere e vendere i propri prodotti e/o servizi. La Divisione Cyber Security di INSIDE svolge quindi attività di prevenzione e sicurezza su tutti gli applicativi web di cui le aziende sono munite.

L'intervento prevede una scansione ed un monitoraggio di tutte le sezioni presenti sull'applicativo web, con una particolare attenzione a quelle protette da username e password che, se bucate, permetterebbero l'accesso ai servizi offerti tramite i protocolli HTTP o HTTPS.

L'intervento coinvolge i seguenti campi di sicurezza:

- scansione dei dati sensibili inviati tramite l'applicativo, esposti al rischio di intercettazione da parte di malintenzionati, tramite l'esame del codice HTML, degli script o di altre informazioni ottenibili da eventuali meccanismi di debugging;
- approfondita analisi dei campi interattivi tra l'applicazione e l'utente, in modo da individuare eventuali falle create da input (in)volontariamente inseriti;
- procedure di autenticazione;
- risoluzione di problematiche relative ad una specifica sessione, come ad esempio timeout, logout, hijacking, login tramite indirizzi non verificati, etc.
- validazione ed alterabilità dei dati;
- esecuzione di comandi in zone impreviste dell'applicazione, che ad esempio, tramite specifiche stringhe SQL, possono portare alla diretta manipolazione del DataBase, con possibilità di acquisizione, modifica, cancellazione dei dati presenti;
- interazioni inappropriate o non corrette con il Sistema Operativo (shell escare).

Threat Detection & Analysis

Proteggi la tua azienda da eventuali dispositivi hardware o software ostili (come virus) che potrebbero danneggiare o inoltrare verso l'esterno i dati sensibili attraverso la nostra procedura di controllo e verifica. Contattaci adesso per una consulenza gratuita.

Computer Hacking Forensics

La generazione digitale sta cambiando il mondo del lavoro. Sempre più spesso le aziende utilizzano nuove tecnologie come il cloud computing, il mobile, i big data o l'IoT rendendole sempre più vulnerabili agli attacchi informatici. Risulta dunque fondamentale sapere se le proprie informazioni siano state manipolate o siano in qualche modo monitorate. Le attività di Computer Hacking Forensics condotte da INSIDE individuano le tracce di un'eventuale intrusione raccogliendo correttamente le fonti di prova necessarie a documentare l'accaduto.

Controspionaggio informatico

INSIDE rileva il grado di **vulnerabilità dei sistemi informatici** dei propri cliente e, a seguito di un'attenta analisi diagnostica, individua gli **interventi idonei alla messa in sicurezza della proprietà informatica**.

Per fornire il miglior supporto possibile, INSIDE ha riunito le migliori competenze nel campo della sicurezza, offrendo servizi di consulenza specifica per l'esecuzione di ogni attività di analisi, con l'obiettivo di proteggere il patrimonio più importante ovvero il **know how aziendale**.

Al giorno d'oggi le modalità per reperire informazioni illecite sono in costante espansione. La rivoluzione digitale ha favorito la nascita del cd. spionaggio informatico colpendo i singoli, ma ancor più frequentemente, le aziende. Come tutelarsi? La parola d'ordine è **prevenzione**.

INSIDE grazie a scrupolose indagini di controspionaggio, individua e elimina il pericolo, svelando eventuali azioni di spionaggio.