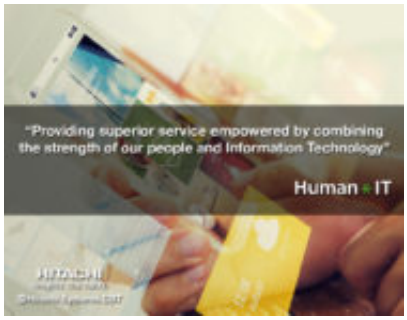
# La sicurezza nell’era del Web Application 2.0: mettere in sicurezza lo sviluppo del Software Enterprise con Hitachi

**Author :** Redazione

**Date :** 22 ottobre 2018




Il lancio di un nuovo servizio è oggi guidato quasi esclusivamente dalle logiche del business, con la conseguenza che i software sono messi a punto in tempi molto rapidi, senza che ci sia la possibilità di delineare chiaramente i requisiti di base e di affrontare i problemi legati alla sicurezza, per i quali spesso si ricorre a pacchetti preconfezionati che si dimostrano poco sicuri perché incompleti o non disegnati sulle caratteristiche del software o dell’azienda, aumentando così il rischio di attacchi esterni.

Trovare e correggere eventuali problemi richiede un investimento importante di risorse e competenze: sarebbe quindi preferibile evidenziare eventuali anomalie in fase di disegno, ma mancano spesso gli strumenti, l’attenzione e la cultura adeguati per intervenire, con il risultato che nella maggior parte dei casi si sottovaluta il reale rischio.

Secondo un’analisi del SANS Institute, “2017 State of Application Security: Balancing Speed and Risk”, il 15% delle aziende esaminate ha dichiarato di aver subito negli ultimi 2 anni un *breach* collegato alle applicazioni.

Per mitigare i rischi di possibili attacchi bisognerebbe delineare e stabilire i requisiti di sicurezza fin dalle primissime fasi di progettazione, tenendo in considerazione diversi fattori: eventuali attacchi esterni a opera di hacker o gruppi organizzati, tentativi di frodi, diffusione di informazioni riservate e comportamenti più o meno leciti perpetrati dai competitor, tipologia di dati utilizzati.


Hitachi Systems CBT propone a tal proposito un approccio programmatico al tema della sicurezza applicativa, basato su un ciclo di vita strutturato in quattro fasi, ognuna della quali è valutabile e ripetibile nel tempo: la prima è la fase di Governance, durante la quale si stabiliscono gli obiettivi del futuro software, si acquisisce consapevolezza del lavoro che si sta progettando; segue la fase di Progettazione, dove devono essere definiti i requisiti di sicurezza necessari; la terza fase è quella della Verifica durante la quale il disegno è analizzato e sottoposto a security test e l'ultima fase, quella Implementativa, si concentra sul controllo applicativo di sicurezza.

Questo ciclo di vita può essere facilmente misurato secondo alcuni fattori e, come tale, può raggiungere diversi livelli di maturità: a fronte dell'implementazione del ciclo è quindi necessario capire se esso abbia raggiunto un livello di maturità consono. I livelli di maturità sono tre: quello iniziale prevede la comprensione e l'utilizzo del modello, il secondo un aumento dell'efficienza e l'ultimo una gestione completa.

Una volta applicato questo modello bisogna valutare costantemente lo stato dell'arte per individuare una *road map* da seguire e implementare passo dopo passo, e capire in definitiva quanto possa essere realizzato.

Hitachi Systems CBT ha concretamente realizzato questo ciclo di vita per **HBG Gaming**, uno dei più grandi operatori italiani presenti nel panorama del gioco sicuro e legale regolato

dall’Agenzia delle Dogane e dei Monopoli. E’ un’azienda certificata ISO 27001 e come tale ha un sistema di gestione della sicurezza che deve tenere in considerazione tutti i controlli imposti dallo standard.

L’intervento di Hitachi Systems CBT si è reso necessario in quanto spesso i fornitori esterni che hanno sviluppato i *software enterprise* utilizzati in HBG Gaming non sono stati in grado di fornire prove adeguate riguardo la gestione delle vulnerabilità nei loro prodotti.

Grazie al ciclo di vita per la gestione della sicurezza applicativa messo a punto dal system integrator del gruppo Hitachi, l’azienda ha individuato le vulnerabilità nei codici sorgenti sin dalle prime fasi progettuali, riuscendo così a dimezzare il TCO – Total Cost of Ownership – grazie ad un pronto intervento nella corretta risoluzione dei problemi.

https://www.youtube.com/watch?v=J6q1YbU6DXg

Maggiori informazioni: www.hitachi-systems-cbt.com

A cura di:

**Marcello David**, Responsabile Sicurezza e Compliance ICT di HBG Gaming
**Michele Onorato,** Security Office Manager di Hitachi Systems CBT