5.5 Sicurezza dei Web Application Server

Il componente estende l'analisi sulla sicurezza dei sistemi informativi che adottano tecnologia web based.

5.5.1 Architettura

Isolamento dei sistemi critici	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	I sistemi critici come i Web Server devono avere un ambiente di elaborazione dedicato, strettamente controllato e monitorato. Tipicamente è necessaria una protezione perimetrale fisica (CED) e logica (firewall). Il web Server va collocato in un segmento di rete di front-end isolato tramite regole firewall dagli altri segmenti interni.

Failover	
Minaccia	Negazione dei servizi.
Contromisure	Prevedere meccanismi di failover del sistema. Ad es. alimentatori, ventole, schede di rete e hard disk devono essere in configurazione ridondata. I sistemi middleware più critici dal punto di vista della disponibilità devono utilizzare meccanismi di clustering applicativo. I sistemi di front-end web più critici per la disponibilità o particolarmente impegnati per un elevato numero di connessioni devono usare meccanismi di clustering applicativo oppure devono essere posti alle spalle di sistemi di bilanciamento del carico. In tutti i casi, in presenza di un fault di un sistema, deve essere presente un processo di controllo (watchdog) in grado di rilevare il fault, generare un alert verso i sistemi di monitoraggio e gestire il carico esistente attraverso gli altri sistemi, eventualmente attivando sistemi di riserva configurati in modalità "hot-standby".

Protezione dei servizi web	
Minaccia	Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Laddove sia necessario pubblicare in front-end web una serie di servizi che risiedono su molteplici server della rete interna, anziché esporre tutti questi server verso l'esterno è necessario invece installare un unico sistema di front-end opportunamente hardenizzato e posizionato su un segmento di rete dedicato, protetto dal firewall perimetrale e controllato da una sonda di intrusion detection. Tale sistema conterrà un servizio di "reverse proxy" o "portale" in grado di presentare in un'unica interfaccia l'insieme dei vari servizi interni, in modo controllato. Su tale sistema è necessario definire opportune politiche di controllo accessi e di autorizzazione, per consentire l'accesso alle varie sezioni del sito (corrispondenti ai diversi servizi interni) ai soli utenti autorizzati.

Sicurezza nelle connessioni nei sistemi web	
Minaccia	- Accesso non autorizzato alle informazioni. - Accesso non autorizzato al sistema. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni.
Contromisure	L'eventuale reverse proxy o portale di front-end deve essere configurato in modo da