5.8 Sicurezza dei Enterprise Service Bus (ESB)

5.8.1 Architettura

Isolamento dei sistemi critici	
Minaccia	- Accesso non autorizzato alle informazioni. - Negazione dei servizi.
Contromisure	I sistemi critici come l'ESB devono avere un ambiente di elaborazione dedicato, strettamente controllato e monitorato. Tipicamente è necessaria una protezione perimetrale fisica (CED) e logica (firewall). Occorrono in linea di principio: - un "external ESB" collocato in DMZ che agisce come Security Gateway (Security Enforcement Point – es. gestione identità) e un "internal ESB" opportunamente messo in sicurezza (vedi best practices successive) a cui l'"external ESB" passa le chiamate esterne e da cui riceve le risposte (ed eventuali chiamate verso l'esterno). Oltre al routing dei messaggi, è qui che avviene la conversione dei messaggi ed è qui che risiedono i business workflow. - Un "Security Decision Service", interno (ossia non in DMZ), cui i 2 ESB si riferiscono come repository unico delle security policies.

5.8.2 Hardening

Hardening del sistema operativo che ospita l'ESB	
Minaccia	- Accesso non autorizzato al sistema. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Eseguire l'hardening del sistema operativo che ospita l'ESB [rif. 5.2.2]. Tipicamente è necessaria una protezione perimetrale fisica (CED) e logica (firewall).

Hardening della piattaforma web che ospita l'ESB	
Minaccia	- Accesso non autorizzato al sistema. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Siccome SOA sfrutta e si basa sulle tecnologie Web, le vulnerabilità associate a tali tecnologie influenzano anche SOA. Pertanto, deve essere eseguito l'hardening della piattaforma web che ospita l'ESB [rif. 5.3.2].

Hardening del Web Services Layer	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate.
Contromisure	Utilizzare adeguati meccanismi di controllo dell'accesso per separare "operazioni interne" da "operazioni esterne" come: - un firewall XML che "tagli" le operazioni interne o - spostare le operazioni interne su servizi Web privati e ospitarle sui server Web interni. Il WSDL di un Web Service pubblica le sue operazioni, i parametri e le associazioni di