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

	rete. Alcune di queste (operazioni interne) devono essere utilizzate solo dal fornitore di servizi, tipicamente le operazioni amministrative. Il resto delle operazioni (operazioni esterne) può essere richiamato dal consumatore di servizi. Ora un attaccante può tentare di indovinare le operazioni interne e invocarle tramite l'endpoint (che è disponibile nel WSDL). Tale attacco è chiamato scansione WSDL.

Hardening del Web Services Layer	
Minaccia	Compromissione delle comunicazioni.
Contromisure	Verificare l'autenticità dei metadati del servizio Web (si tenga presente che non esistono meccanismi standard per verificare l'autenticità dei metadati). Un attaccante che, ad esempio, riesca a modificare l'endpoint del servizio può mettere in atto un man-in-the-middle attack per l'intercettazione o la modifica dei dati del servizio Web.

Hardening del Web Services Layer	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	La validazione dello schema del contenuto cifrato va eseguita dopo la decifratura e non prima. Gli standard di XML Encryption e XML Signature, utilizzati per fornire servizi di crittografia e firma digitale sui messaggi scambiati via Web Services (ad esempio SOAP), possono essere utilizzati da un attaccante per nascondere codice malevolo che va in esecuzione durante la decifratura (Attack obfuscation).

Hardening del Web Services Layer	
Minaccia	Negazione dei servizi.
Contromisure	Le richieste dei service consumer devono essere elaborate solo se gli elementi del security header del messaggio SOAP in entrata corrispondono esattamente ai requisiti imposti dallo schema della security policy. Diversamente vanno scartati. Lo standard WS-Security non impone restrizioni né su quali parti del security header di un messaggio SOAP possono essere crittografate né sulla dimensione massima di un messaggio crittografato. Ciò significa che un attaccante è in grado di provocare un denial of service inviando a un servizio Web dei security headers crittografati di grandi dimensioni. Le operazioni di decifratura causano un carico elevato sulla CPU del server che ospita il Web Service, carico che a sua volta crea problemi di disponibilità.

Hardening del Business Processes Layer	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate.
Contromisure	Estendere i meccanismi di controllo dell'accesso per separare “operazioni interne” da “operazioni esterne” a livello BPEL. Un WS-BPEL (BPEL) di un processo di business può essere sottoposto ad un attacco di "BPEL scanning" analogo al “WSDL scanning” (ma portato su un layer diverso).

Hardening del Business Processes Layer	
Minaccia	Compromissione delle comunicazioni. - Metadata spoofing
Contromisure	Verificare l'autenticità dei metadati a livello BPEL. Un attaccante, ad esempio, potrebbe modificare a suo vantaggio i riferimenti di endpoint del processo aziendale nella dichiarazione BPEL.

BPEL state deviation	
Minaccia	Negazione dei servizi. - Metadata spoofing
Contromisure	Un attaccante può inondare (flood) il motore BPEL con molti messaggi BPEL che sono conformi allo schema ma non hanno alcun contenuto significativo. Le risorse computazionali del motore BPEL potrebbero esaurirsi producendo un attacco di denial of service. Per rifiutare i messaggi non validi, l'approccio migliore è quello di utilizzare un application level firewall.

Hardening del Business Processes Layer	
Minaccia	Negazione dei servizi - Instantiation flooding (diretto e indiretto)
Contromisure	I motori BPEL istanziano un nuovo processo quando ricevono un "receive message" (che istanzia un processo BPEL). Quando viene ricevuto un "receive message", il motore BPEL sospende l'esecuzione corrente finché il messaggio entrante è completamente ricevuto. Un attaccante può sfruttare questo comportamento dei motori BPEL inondandoli di "receive message" non validi, producendo un attacco di denial of service. L'attacco può avvenire anche in modo indiretto: si colpisce un motore BPEL per attaccarne un altro che interagisce con il primo. La protezione dei motori BPEL contro questa tipologia di attacchi di flooding è complessa: occorrerebbe un'analisi semantica per individuare i messaggi non validi. E ciò esula dalle possibilità di un application level firewall. In caso di attacco occorre intervenire a livello di difesa perimetrale in modo mirato.

Hardening del Business Processes Layer	
Minaccia	Compromissione delle comunicazioni - WS-Addressing spoofing
Contromisure	Verificare la validità degli endpoint prima che il processo venga eseguito dal motore BPEL (caso di endpoint non validi o pericolosi) La specifica WS-Addressing descrive come indirizzare in modo standard gli endpoint di un web service o di un business process. Un attaccante può modificare gli header WS-Addressing facendo puntare il motore BPEL agli endpoint di servizi o di processi non validi o pericolosi.

Hardening del Business Processes Layer	
Minaccia	Negazione dei servizi - Workflow engine hijacking
Contromisure	Verificare la validità degli endpoint prima che il processo venga eseguito dal motore BPEL (caso di endpoint a un sistema di destinazione esistente, che fornisce un servizio reale all'URL specificato). In caso contrario, un attaccante può utilizzare il WS-Addressing spoofing per provocare il denial of service di un servizio legittimo attraverso un attacco di flooding. L'endpoint di cui l'attaccante esegue lo spoofing è quello di un servizio legittimo (il target dell'attacco). Il sistema attaccato tenta di elaborare una grande quantità di messaggi che gli pervengono come risultato del WS-Addressing spoofing e, se non ci riesce, i suoi utenti legittimi subiscono un Denial of Service.

Hardening del protocollo SOAP	
Minaccia	Attacchi all'integrità dei sistemi - Harmful SOAP attachments
Contromisure	I messaggi SOAP possono contenere allegati di dimensione arbitraria. Pertanto un

	attaccante può allegare un virus a un messaggio SOAP e inviarlo per l'elaborazione al sistema di destinazione. Gestire gli allegati SOAP secondo le seguenti modalità: - bloccarli se non previsti o sospetti; - filtrarli in base al MIME-type; - analizzarli con un anti-malware.

Hardening del protocollo SOAP	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - Negazione dei servizi. - (SOAPAction spoofing).
Contromisure	Verificare rigorosamente se l'azione specificata nel SOAP body corrisponde all'azione specificata nell'HTTP header. Se non corrispondono, il messaggio in arrivo deve essere rifiutato. Non utilizzare mai il campo SOAPAction nell'intestazione HTTP come identificativo dell'operazione del servizio. Un malintenzionato potrebbe facilmente modificare l'elemento "SOAPAction" nell'intestazione HTTP per eseguire un'azione diversa da quella specificata nel SOAP body.

Hardening dei documenti XML	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - (XPath injection).
Contromisure	È necessario utilizzare un'interfaccia XPath parametrizzata (se disponibile) oppure eseguire la sanitizzazione dell'input utente prima di includerlo in una query costruita dinamicamente (in analogia con le tecniche per evitare la SQL Injection). La specifica XPath viene utilizzata per navigare nel contenuto di un documento XML. Un attacco di XPath injection (simile all'attacco SQL injection) inietta un'espressione XPath all'interno di quella predisposta dal programmatore al fine di accedere a informazioni non autorizzate in un documento XML.

Hardening dei documenti XML	
Minaccia	Negazione dei servizi.
Contromisure	Limitare la dimensione dei messaggi SOAP in arrivo per contrastare un attacco di payload di grandi dimensioni. Si tenga presente che l'approccio Document Object Model (DOM) per l'analisi e l'elaborazione di XML consuma una grande quantità di memoria. Ciò è dovuto al fatto che è necessaria una rappresentazione in memoria ad oggetti dell'intero documento XML, che richiede molto più spazio di memoria rispetto al documento XML stesso. Payload di grandi dimensioni possono essere ottenuti ad esempio: - Abusando della proprietà di nesting di elementi, inserendo a piacimento molteplici elementi nel documento. - Abusando della funzionalità di DTD (Document Type Definitions) per creare ricorsivamente entità all'interno del documento fino a farlo "esplodere".

Hardening dei documenti XML	
Minaccia	Negazione dei servizi.
Contromisure	Considerare l'impiego di session tokens univoci nei messaggi SOAP come i nonces