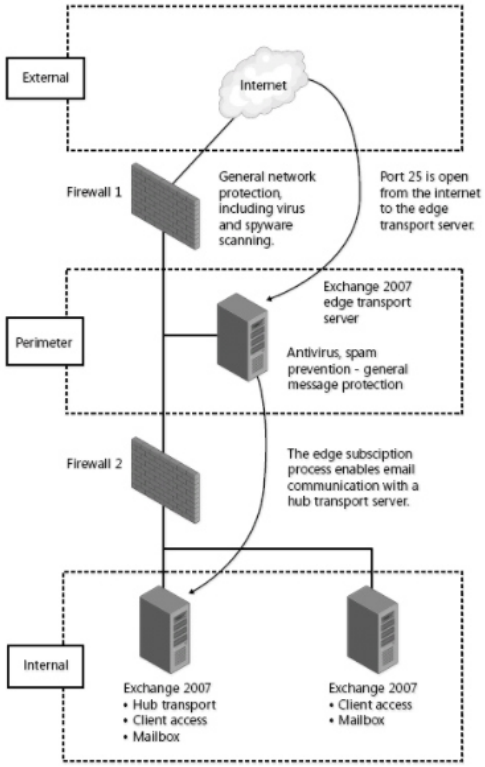
Oracle Database 12c	Per informazioni aggiornate sulle impostazioni di protezione e privacy per Oracle Database 12c, scaricare il documento: http://www.oracle.com/us/products/database/securing-oracle-database-primer-2522965.pdf.
Microsoft SQL Server 2012	Per informazioni aggiornate sulle impostazioni di protezione e privacy per Microsoft SQL Server 2012, visitare il sito: https://docs.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server.

5.7 Sicurezza del Mail Server

5.7.1 Architettura

Isolamento dei sistemi critici	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	I sistemi critici come il Mail Server 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 SMTP server hardenizzato collocato in DMZ che si limita ad accettare le connessioni in ingresso provenienti da Internet, con funzione di "relay"; - uno o più mail server interni anch'essi opportunamente messi in sicurezza (vedi best practices successive) a cui l'SMTP server in DMZ inoltra (relay) le mail ricevute dall'esterno e da cui riceve quelle provenienti dall'interno. Inoltre si può considerare di installare un Application Layer inspection firewall a protezione del server SMTP in DMZ. Si consideri, a titolo di esempio, il seguente schema (con 2 firewall) in ambiente Microsoft:  [Fonte: https://msdn.microsoft.com/en-us/library/cc505927.aspx]

Failover	
Minaccia	Negazione dei servizi.
Contromisure	Prevedere meccanismi di failover dei sistemi di posta elettronica.

Controllo del traffico dati	
Minaccia	- Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Negazione dei servizi.
Contromisure	Attivare, a livello perimetrale, un dispositivo di sicurezza intelligente di tipo IDS (Intrusion Detection System) o IPS (Intrusion Prevention System) per individuare (IDS) la presenza di codice malevolo e bloccare (IPS) le intrusioni.

Hardening del MailServer	
Minaccia	- Accesso non autorizzato alle informazioni. - Accesso non autorizzato ai sistemi. - Negazione dei servizi.
Contromisure	Concedere al Mail Server i privilegi minimi necessari per completare le operazioni richieste. In particolare i processi del server devono essere eseguiti nel contesto di una utenza non privilegiata.

Hardening del MailServer	
Minaccia	- Accesso non autorizzato ai sistemi. - Compromissione delle comunicazioni.
Contromisure	Customizzare opportunamente le configurazioni di base del mail server. In particolare, cambiare i nomi degli account di default e degli alias pre-definiti.

Hardening del MailServer	
Minaccia	Negazione dei servizi.
Contromisure	Configurare le applicazioni, i servizi e il sistema operativo tenendo sempre presente le possibili esposizioni ad attacchi DoS. Assicurarsi che i criteri di blocco dell'account predisposti non possano essere sfruttati per bloccare service accounts ben noti. Assicurarsi che il sistema sia in grado di gestire alti volumi di traffico e che le soglie siano opportunamente impostate per gestire carichi anormalmente elevati.

Hardening del MailServer	
Minaccia	- Compromissione delle comunicazioni. - Negazione dei servizi.
Contromisure	L'utilizzo di black-list di IP/indirizzi mail costruite sulla base di osservazioni su attacchi avvenuti in passato, può ridurre notevolmente i rischi derivanti da attacchi di vario tipo (es. spam). Tali liste sono disponibili in internet oppure sono incluse in prodotti commerciali di protezione dei mail server. Ove possibile, limitare gli accessi a indirizzi IP/indirizzi mail presenti in queste black-list.

Hardening del MailServer	
Minaccia	Divulgazione di informazioni riservate.

Contromisure	Configurare opportunamente i messaggi prodotti dal mail server (messaggi di Hello, risposte automatiche ad es. per i messaggi non consegnabili, messaggi di errore, funzionalità diagnostiche, ecc.) in modo da non rivelare nessuna informazione ad un eventuale aggressore, quali ad es. indirizzi email degli amministratori o di altri utenti o di caselle di risposta automatica, versione del software, ecc. Infatti un malintenzionato potrebbe indurre il sistema in errore per ottenere indirizzi email validi da usare ad es. in una campagna di phishing o spamming.

Hardening del MailServer	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Attacchi all'integrità dei sistemi (software e configurazioni). - Furto di credenziali di autenticazione (es. keylogger). - Negazione dei servizi. - Tentativi di frode. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Filtrare gli Attachments. Installare un software antivirus e implementare filtri per bloccare attachment sospetti o potenzialmente pericolosi.

Hardening del MailServer	
Minaccia	- Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni.
Contromisure	Utilizzare solo protocolli sicuri per l'accesso alla posta elettronica: - Client POP3: Solo se si utilizza con SSL/TLS, altrimenti usare IMAP4. - Client IMAP4: Configurare sempre l'uso di SSL/TLS. - Server SMTP: Configurare sempre l'uso di SSL/TLS. Utilizzare solo TLS 1.2, evitando SSL e le versioni precedenti di TLS, in quanto vulnerabili a diverse tipologie di attacchi.

Hardening del MailServer	
Minaccia	- Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni.
Contromisure	Webmail Access. Se il MailServer supporta la Webmail, è necessario adottare tutte le misure di sicurezza previste nel presente documento per i server web. In particolare però il server di webmail deve obbligatoriamente utilizzare HTTPS con TLS 1.2 o superiore, per l'intera durata della sessione.

Hardening del MailServer	
Minaccia	Negazione dei servizi.
Contromisure	Limitare sempre la dimensione massima dei messaggi e degli attachments sia per i messaggi in ingresso sia per quelli in uscita, utilizzando valori considerati accettabili per l'organizzazione. Ciò protegge da situazioni potenzialmente pericolose (degrado prestazioni, crash, esaurimento disco, SPAM e attacchi DOS verso terzi) in cui messaggi con allegati di grandi dimensioni sono inviati a molteplici destinatari. Configurare anche un numero massimo ragionevole di destinatari per i messaggi in uscita o in fase di relay. Configurare una dimensione massima ragionevole per le mailbox degli utenti e per le