5.6.2 Hardening

Hardening della piattaforma DBMS	
Minaccia	- Accesso non autorizzato alle informazioni. - Accesso non autorizzato ai sistemi. - Negazione dei servizi. - Uso non autorizzato di privilegi.
Contromisure	Concedere al DBMS i privilegi minimi necessari per completare le operazioni richieste. In particolare i processi del DB devono essere eseguiti sul sistema nel contesto di una utenza non privilegiata (diversa da root/Administrator e dotata dei privilegi minimi necessari). Disinstallare o disabilitare tutte le componenti opzionali / aggiuntive del DBMS non strettamente necessarie (es. Reporting Services, Debugging, interfacce amministrative, servizi di replica o backup, servizi di ricerca Full Text, interfacce web o Web Services, ecc.). Prestare particolare attenzione a quelle componenti aggiuntive che espongono servizi o interfacce amministrative su specifiche porte TCP/IP. Rimuovere gli "schema" e i DB di default presenti al termine dell'installazione standard e non utilizzati. Dopo la creazione del database, rimuovere gli eventuali script utilizzati per la creazione o, come minimo, spostarli su un repository "sicuro" (quanto meno dotato di controllo accessi) ed esterno al sistema. Quando si avviano processi o tools legati al DBMS, evitare di fornire a linea di comando informazioni sensibili quali ad es. username e password o chiavi crittografiche, perché tali parametri possono essere visualizzati da tutti gli utenti del sistema, anche in remoto, esaminando l'elenco dei processi in esecuzione. Analogamente, tali informazioni non devono essere memorizzate neppure in variabili d'ambiente né come testo in chiaro in file batch, ma piuttosto fornite a mano dall'operatore, o memorizzate in file di configurazione crittografati o come minimo offuscati. I file temporanei prodotti dal processo di installazione che possono contenere password devono essere rimossi.

Hardening della piattaforma DBMS	
Minaccia	Abuso di risorse.
Contromisure	Disabilitare gli script, le applicazioni d'esempio, le utility non strettamente necessari ed ogni altra funzionalità non pertinente agli scopi della piattaforma DBMS, proposti dalle configurazioni di base del DBMS.

Protezione delle informazioni strumentali all'accesso	
Minaccia	Accesso non autorizzato ai sistemi.
Contromisure	Non utilizzare nomi di account predefiniti e rinominare account standard come l'account amministratore del DB. Non utilizzare password nulle. Tutti gli accessi al sistema operativo e ai server di database, avvenuti con o senza successo, devono essere registrati. I log contenenti tali informazioni devono essere conservati per almeno un anno. Gli oggetti del database contenenti dati con particolari restrizioni, lì dove tecnicamente possibile, devono essere predisposti per l'auditing. I dati di log devono essere regolarmente esaminati da persone esperte e indipendenti designate dal titolare dei dati per soddisfare le proprie esigenze. Tali requisiti e il processo di revisione devono essere ben documentati. Eseguire l'Audit degli accessi non andati a buon fine per intercettare tentativi di indovinare le password.

Accesso a dati sensibili su memoria di massa	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	Utilizzare ACL restrittive per tutti i data stores e in particolare per quelli che contengono dati sensibili. Memorizzare i data store che contengono dati sensibili o comunque riservati su file system crittografati.

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

Hardening del sistema operativo che ospita il DBMS	
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.
Contromisure	Eseguire l'hardening del sistema operativo che ospita il DBMS. L'hardening del sistema operativo è oggetto di un paragrafo specifico [rif. 5.2.2].

Patching del DBMS	
Minaccia	- Accesso non autorizzato al sistema. - Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Eseguire il patching iniziale (prima di mettere in uso i sistemi DBMS) e successivamente in maniera regolare e periodica, installando tutti gli aggiornamenti suggeriti e di sicurezza rilasciati dal produttore. Verificare che la versione del software del database sia attualmente supportata dal fornitore o dal progetto open source, come richiesto dagli standard minimi di sicurezza. Il software del database deve essere aggiornato per includere tutte le patch di sicurezza ultime. Predisporsi per applicare le nuove patch di sicurezza in modo tempestivo.

Disabilitazione delle interazioni con il sistema operativo	
Minaccia	- Accesso non autorizzato al sistema. - Attacchi all'integrità dei sistemi (software e configurazioni). - Compromissione delle comunicazioni. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Molti DBMS, tra cui Microsoft SQL Server (attraverso alcune Extended Stored Procedure come *xp_cmdshell*, *xp_dirtree*, *xp_servicecontrol*, ecc.) e Oracle (con altri meccanismi) consentono di interagire in modo molto stretto con il sistema operativo, ad es. richiamando eseguibili sul sistema, navigando sul file system, avviando/arrestando servizi o eseguendo altre operazioni anche privilegiate. Tali meccanismi, quando non effettivamente necessari, devono essere disabilitati.