Transparent Database Encryption (TDE)

Rövid leírás:
Lehetővé teszi az SQL szervert, hogy az adat a szerver merevlemezére való írása során kerüljön titkosításra, és az SQL szerver visszafejti ahogy a merevlemezről olvas a memóriába.
Ez a titkosítás a blokkokban tárolt adatok helyett az adatblokkok titkosításával történik.
A két fogalom között az a különbség, hogy az adatok titkosítása során csak a táblán belüli adatokat titkosítják, míg a TDE titkosítja a táblák metaadatait, az ún. white space-eket, stb..

Előnyök:
Úgy titkosíthatunk adatot, hogy az adat semmilyen formában nem változik meg.
A tartalék mentett (backup) verzió is titkosított.
Egyszerű a metódus bekapcsolása.

Hátrányok:
Ha valaki hozzáfér az SQL szerverhez SQL injection használatával vagy normál módon, az képes lesz letölteni az adatbázis adatait egy egyszerű lekérdezéssel.
Az SQL szerver CPU terhelését is növeli, mivel minden egyes lemezre írt vagy olvasott adatot titkosítani kell. Nagy terhelésű rendszereken ez a CPU erőforrásainak nagy növekedését jelentheti.

Column-Level Encryption

Rövid leírás:
Kiválaszthatjuk, hogy melyik oszlopokat szeretnénk titkosítani a teljes fájl titkosítása helyett.

Előnyök:
Könnyedén elkülöníthető az érzékeny és nem érzékeny adat egymástól.
Külön kulcs használható minden oszlop titkosítására, így a biztonság növekszik.

Hátrányok:
Külön kulcsok használata miatt ezeknek az oszlopához való hozzáférési idő növekszik az egyszerű szövegéhez képest. Minél több a titkosított oszlop, annál magasabb a potencionális teljesítmény csökkenés.

Field-Level Encryption / Cell-Level Encryption

Rövid leírás:
Kiválaszthatjuk, hogy melyik mezőt szeretnénk titkosítani a teljes fájl vagy oszlop titkosítása helyett.

Előnyök:
Könnyedén elkülöníthető az érzékeny és nem érzékeny adat egymástól.
Külön kulcs használható minden mező titkosítására, így a biztonság növekszik.

Hátrányok:
Külön kulcsok használata miatt ezeknek a mezőihez való hozzáférési idő növekszik az egyszerű szövegéhez képest. Minél több a titkosított mező, annál magasabb a potencionális teljesítmény csökkenés.

Application-Level Encryption / Application Layer Encryption

Rövid leírás:
Az alkalmazáson belül titkosítja az adatot.
A titkosítandó adattal foglalkozó program végzi a kódolási folyamatot.

Előnyök:
Könnyen megoldható a titkosítási folyamat.
Az adat csak a megfelelő alkalmazáson keresztül érhető el.
A megfelelő alkalmazás irányítja a kulcs-igazgatást (key-management) .

Hátrányok:
Kulcs-igazgatás (key-management) nehéz.
Titkosított szövegben kell keresni.
Könnyedén implementálható, de nehezen tökéletesíthető módszer.

Data Encryption Standard (DES)

Rövid leírás:
Blokk-titkosító folyamat, az adatokat 64 bites blokkokban enkriptálja. 64 bit nagyságú sima szöveg titkosítás után 64 bites titkosított szöveg lesz.
56 bit nagyságú kulcs.

Előnyök:
Bonyolult, hosszas matematikai számításokat végez, így a kód feltörése nehéz. (16 kör egy matematikai folyamatból)

Hátrányok:
Titkosítás és visszafejtés ugyanazzal az algoritmussal és kulccsal történik.

Triple DES

Rövid leírás:
Működése megegyezik a DES működésével, viszont 3x16 kör a titkosítási folyamat.

Előnyök:
Biztonságosabb mint a DES a hosszabb titkosítási folyamat miatt.

Hátrányok:
Titkosítás és visszafejtés ugyanazzal az algoritmussal és kulccsal történik.

Advanced Encryption Standard (AES)

Rövid leírás:
Egy blokk mérete 128 bit. 128/192/256 bit nagyságú kulcs.
Több fázisból áll. Bonyolult algoritmus.
Kulcs méretétől függ, hogy hányszor fog az algoritmus az adott blokkon végrehajtódni (128 – 10x, 192 – 12x, 256 – 14x).

Előnyök:
Bonyolultsága és kulcs nagysága miatt nehezen feltörhető.
Bevált módszer, egész világon használják.

Hátrányok:
Szoftveresen nehezen implementálható.
Ha sikerül a szoftveres megvalósítás teljesítményi ideje valószínűleg elég nagy lesz.
Minden blokk ugyanazon módon lesz titkosítva.

Összehasonlítási szempontok

Mikor / hol használják főleg

-TDE: Főleg akkor használják amikor éppen nem használt adatot (data-at-rest) akarnak titkosítani.
-Column-LE: Amikor pontosan be tudjuk kategorizálni, hogy melyik adat szenzitív és melyik nem.
-Field-LE: Amikor pontosan be tudjuk kategorizálni, hogy melyik adat szenzitív és melyik nem.
-Application-LE: Ha nem akarunk a mögöttes rétege szállítási/data-at-rest titkosítására támaszkodni.
-DES: Nem igazán használják már, a gyengeségeit már felfedezték.
-Triple-DES: Komplexebb mint a DES ezért ezt még használják, de ettől függetlenül ugyanazon problémái megvannak mint a DES-nek.
-AES: Világszerte mindenütt használják, a legbiztonságosabb titkosítási módszerként ismert.

Idő / gyorsaság

-TDE: Lassabb
-Column-LE: Lassabb.
-Field-LE: Lassabb.
-Application-LE: Biztonságos.
-DES: Gyorsabbnak mondható.
-Triple-DES: Hasonló a DES-hez.
-AES: Lassú.

Biztonság / hatékonyság

-TDE: Biztonságos.
-Column-LE: Biztonságos.
-Field-LE: Biztonságos.
-Application-LE: Biztonságos.
-DES: Kevésbé biztonságos, már rájöttek feltörési módjaira.
-Triple-DES: Biztonságosabb mint az elődje, a DES.
-AES: Nagyon biztonságos.