Infbizt 1

Információbiztonság

Az információbiztonság az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számonkérhetőség, a

letagadhatatlanság és a megbízhatóság, szintén ide tartozhatnak

Fogalmak és célok

-C (bizalmasság): csak azok érhessék el az információt akik arra jogosultak

-I (sértetlenség): védelem az adatok jogtalan módosítása ellen

-A (rendelkezésre állás): az adat vagy szolgáltatás garantált elérhetőségét biztosítja

(hitelesítés, személyes információk védelmezése, letagadhatatlanság)

Alapfogalmak:

-hozzáférés vezérlés: authentication (azonosítás), authorization (jogosultság), (accountability(naplózás)

-fenyegetés

-sebezhetőség

-kockázat

Biztonsági alapelvek

1. A biztonság relatív fogalom, nem lehet önmagában kijelenteni, hogy egy rendszer biztonságos. Mindig attól függ, hogy mi ellen szeretnénk védekezni.

A kockázatmenedzsment feladat, hogy eldöntse mennyi időt, pénzt és energiát érdemes ráfordítani a biztonságra.

2. A jó védelem rétegezett, a védelmet úgy kell kialakítani, hogy sok kontroll védje az értékes rendszert.

3. Változatos legyen a védelem, a rétegek ne legyenek hasonlóak, mert könnyíti a támadó dolgát.

4. Minimalizáljuk a jogosultságokat, tehát mindenki csak annyi jogosultságot kapjon amennyi a feladatainak elvégzéséhez elegendő.

5. Feladatkörök szétválasztása, hogy ne egy ember legyen felelős a fontos dolgokért

6. Implicit tiltás elve, azaz amire nem vonatkozik szabály az alapból legyen TILOS.

7. Nem alapozhatjuk egy rendszer biztonságát arra, hogy a környezetet és a védelmi mechanizmust nem hozzuk nyilvánosságra

8. Minden lánc csak annyit bír amennyit a leggyengébb láncszem tartani tud.

9. Nincs 100% os biztonság rések mindig voltak és lesznek. (Tévedni emberi dolog)

területek

Védelmi kontrollok

Egy rendszer védelmének tervezésekor a követelmények rögzítése után egy védelmi mechanizmust kell létrehoznunk.

1. Megelőző kontroll: tűzfal, megakadályozzák egy adott esemény bekövetkezését

2. Észlelő kontroll: minél hamarabb észleljük a nem kívánatos esemény bekövetkezését.

3. Elhárító kontroll: beavatkozik az esetleges rendellenes események folytatásába.

Kockázatmenedzsment

Kockázat:

Nemkívánatos esemény bekevöetkezésének valószínűsége * a kár mértéke

Fenyegetés:

-az az ember vagy esemény, aki a biztonsági esemény okozója lehet

1. külső fenyegetés: a támadók nem férnek hozzá a rendszer belső erőforrásaihoz

2. belső fenyegetés: a támadó hozzáfér bizonyos belső információkhoz. A támadó célja a jogosultságok kiterjesztése.

3. kihasználás: kihasználjuk a rendszer sérülékenységét

Sérülékenység:

Biztonsági rés, amely gyengesége incidensre vagy katasztrófára ad lehetőséget.

Web-alkalmazások biztonsága.

-OWASP: nyílt független non-profit szervezet, amely az alkamazásbiztonságot előre segíti

1. Injektálás: adatmezőbe futtatható kódot adhatunk meg és ezzel rávesszük az alkalmazást, hogy végrehajtsa az általunk írt utasítást.

SQL injektálás

Védekezés:

-nincs adatbázis

-kódoljuk az adatokat

-SQLinjection ellen: prepared statementek.

2. Hibás felhasználó azonosítás:

A hitelesítő adatok kikövetkeztethetőek vagy felülírhatóak.

Védekezés:

-authentication legyen egyszerű és központosított

-több faktoros hitelesítés

3. Weboldalak közötti szkriptelés

A támadó szkriptet készít melyet a célpont böngészője értelmez és feldolgoz. A sérülékenység abból adódik, hogy az űrlapon keresztül érkező adatokat a böngésző alkalmazás ellenőrzés nélkül jeleníti meg.

Tipikus hatásai:

-adatok ellopás

-weboldal tartalmak átírása

-átirányítás más weboldalra

Védekezés:

-ellenőrizzük a felhasználói bemeneteket biztonságos api-al

-készítsünk fehér listát a lehetséges válaszokról

4. Nem biztonságos direkt objektumhivatkozások

A direkt link birtokában elérhetünk olyan tartalmat amit a felhasználó nem szándékozik megosztani

Védekezés:

-szerver oldalon ellenőrizni a jogosultságot

-temporális értékek generálása a linkbe

5. Helytelen biztonsági beállítások:

Telepítéskor nincs megváltoztatva az alapértelmezett hozzáférés. Rosszul vagy hiányosan konfigurált rendszer. (alapértelmezett jelszavak)

Védekezés:

-telepítési útmutató

-konfiguráció dokumentáció

-automatizáljuk az alkalmazások tesztelését

6. Érzékeny adatok kiszivárgása II.

Az áldozat megadja a hitelkártya számát a weboldalon.

Védekezés:

-az adatok biztonsági osztályokba sorolása (nyilvános, érzékeny, fokozottan érzékeny)

-titkosításhoz használjunk kriptográfiát

7. Hiányzó funkció szintű hozzáférés ellenőrzés

A dinamikusan generált oldalakon jogosultsági szinttől független jeleníthetünk meg tartalmat.

Védekezés:

-implementáljunk szerver oldali ellenőrzést

-tesztelés

-fehér listás engedélyezés

8. Weboldalak közötti kéréshamisítás I.

Egy sérülékeny webalkalmazás nem ellenőrzi, hogy a beérkező kérés szabályos módon keletkezett-e.

Védekezés:

-tokenek, adjunk a tranzakciókhoz egy kiegészítő titkot, amely minden letöltéskor megváltozik

-ha a kéréssel együtt nem kapjuk vissza a generált tokent akkor utasítsuk el a kérést

9. Ismert sérülékenységet tartalmazó komponensek használata

Olyan függvénykönyvtárakat vagy kiterjesztéseket használunk amelyben sérülékenységek lehetnek.

Védekezés:

-automatizált ellenőrzi, amely ellenőrzi a komponensek verzióit valamint riaszt ha sérülékenységet talál

-rendszeresen frissítsük a komponenseket

10. Ellenőrizetlen oldalátirányítások

Az átirányítások dinamikus generálásához használhat olyan paramétert a webapp amit a felhasználó meg tud változtatni, ezzel károkat okozva.

Védekezés:

-ne használjunk átirányítást

-ha használunk akkor ne paraméterből vegyük az átirányítási célt