INFORMATIKAI PROJEKTELLENŐR

DOMBORA SÁNDOR

ADATBÁZISOK ÉS STATISZTIKAI ADATOK VÉDELME

Tartalom

- **Adatbázisok biztonsága**
  - Biztonságtervezési stratégiák
  - Biztonságos kommunikáció
- **Statisztikai adatok védelme**

Biztonságtervezési technikák

MINIMISE

- A stratégia kimondja, hogy az elégséges de lehető legkevesebb személyes adatot szabad csak összegyűjteni.

HIDE

- A stratégia kimondja, hogy a személyes adatokat és kapcsolataikat el kell rejteni az egyszerű betekintés elől.

Biztonságtervezési technikák

SEPARATE

- A stratégia kimondja, hogy a személyes adatat elosztott módon, külön tárolóegységekben kell tárolni, amikor csak lehet.

AGGREGATE

- A stratégia kimondja, hogy a személyes adatokat a lehető legmagasabb aggregálási szinten kell kezelni, amelynek részletei elégségesek a feldolgozáshoz.

Biztonságtervezési technikák

INFORM

- A stratégia a transzparencia elvét támogatja, azaz az érintetteket megfelelően kell tájékoztatni, amikor személyes adatfeldolgozás történik.

CONTROL

- A stratégia kimondja, hogy az érintetteknek kontroll lehetőséget kell nyújtani az adataik feldolgozása során

Biztonságtervezési technikák

ENFORCE

- A stratégia értelmében követni kell a jogi követelmények érvényesülésének elvét. Összefügg a számonkérhetőséggel.

DEMONSTRATE

- A stratégia megköveteli, hogy az adatvédelmi ellenőr képes legyen bizonyítani az adatvédelmi irányelvek és jogszabályok teljesülésért. Összefügg a számonkérhetőséggel.

Biztonságos privát kommunikáció

Biztonságos privát kommunikáció

- Kódolt csatornák
- Gyakori protokollok
  - TLS – Transport Layer Security
  - SSH – Secure Shell
- IPSec – két hálózat közötti titkosított csatorna
- Végpontok közötti titkosítás
- Kulcscserék – munkamenetenként csere
- A metaadat nem titkos – kideríthető ki – kivel beszél

Biztonságos privát kommunikáció

Anonim kommunikáció

- A hívás indítója és fogadója anonim marad
- **Egy átjárós modellek:**
  - Proxy-k: elrejtik a kommunikálót, de felderíthető
  - VPN előfizetés: titkosít egy publikus átjáróig, globális
  - megfigyelő felderítheti a kommunikálót

Biztonságos privát kommunikáció

Több átjárós modellek:

- Onion routing: több lehetséges átjárót használ felváltva a kommunikációhoz, nehezebben deríthető fel globális megfigyelő által
- Mix-hálózatok: a több átjárós modellt használják, az átjárók univerzális csomagokat használnak a statisztikák elfedésére
- Broadcast sémák: Mindenkinek elmegy az üzenet, és mindenkinek meg kell próbálni dekódolni a saját kulcsával - költséges

Titkosítás

Szteganográfia

- Rejtett üzenetek létrehozásának tudománya
- Csak a címzett tud róla
- Az üzeneteket egy „zajos” kép- vagy hangfájl legkisebb helyi értékű bitjeibe rejtjük
- Futtatható programokban való elrejtés
- Null kódolás – szöveg elrejtése szövegben, pl. minden szó első betűje

Tárolók biztonsága

Kontrollok

- Operációs rendszer kontrollok (login)
- Helyi titkosított tároló (teljes lemez, fájlrendszer)
- Fájlrendszer (FSE) – csak a fájlokat titkosítja
  - FileVault
  - TrueCrypt
- Teljes lemez (FDE) – a teljes meghajtót titkosítja
  - BitLocker – AES alapú, TPM
  - LUKS – Linux Unified Key Setup

Adatok biztonsága adatbázisban

Kontrollok

- Titkosított oszlopok
- Titkosított adatsorok
- Virtuális privát adatbázis
  - Egy adatbázis tábláiban több szervezet adatát tárolják
  - Mindenki csak a saját adataihoz fér hozzá

Tárolók biztonsága

Kontrollok

- Formátum megőrző titkosítás (pl. bankkártya szám kódolás után érvényes bankkártya szám lesz)
- Távoli biztonságos lemez – probléma a kulcs elhelyezése
- Titkosított adatok keresése
  - Symmetric Searchable Encription (SSE)
  - Public-key Seachable Encription (PSE)
  - A létrehozott indexek árulkodnak

Statisztikai adatbázisok védelme

Válaszadók védelme

- Egy adott statisztikai lekérdezésbe egy adott kategóriába túl kevés válasz esik
- Akkor szokott elfordulni, ha az adatbázist elérhetik 3. felek számára

Tulajdonos védelme

- Csak a kiszámított statisztika eredménye kerül felfedésre

Felhasználó védelme

- A lekérdezések szférájának védelme a felhasználói profilozással szemben

Statisztikai adatbázisok védelme

Táblázatos adatvédelem

- Frekvencia táblázatok (betegek száma járványonként és városonként)
- Magnitúdó táblázatok (betegek számának átlaga járványonként és városonként)
- Kapcsolt táblák (Közös kategória attribútumok)

Védekezési formák

- Érték elnyomás
- Érték módosítás – kontrollált kerekítés

Mikro adatok védelme

Adatklasszifikálása a nyilvánosság szerint

- Azonosító attribútum
- Kvázi-azonosító attribútum
- Bizalmas eredmény attribútum
- Nem bizalmas eredmény attribútum

Védelmi elvek

- Maszkolás (zaj hozzáadása, pontosság csökkentése, elnyomás)
- Szintetikus adatgenerálás – bizonyos eredeti adattulajdonságok megőrzése

Sérülékenységvizsgálat

Black box vizsgálat

- A vizsgálandó adatbázis, portál vagy alkalmazás elérhetősége kerül átadásra.

Gray box vizsgálat

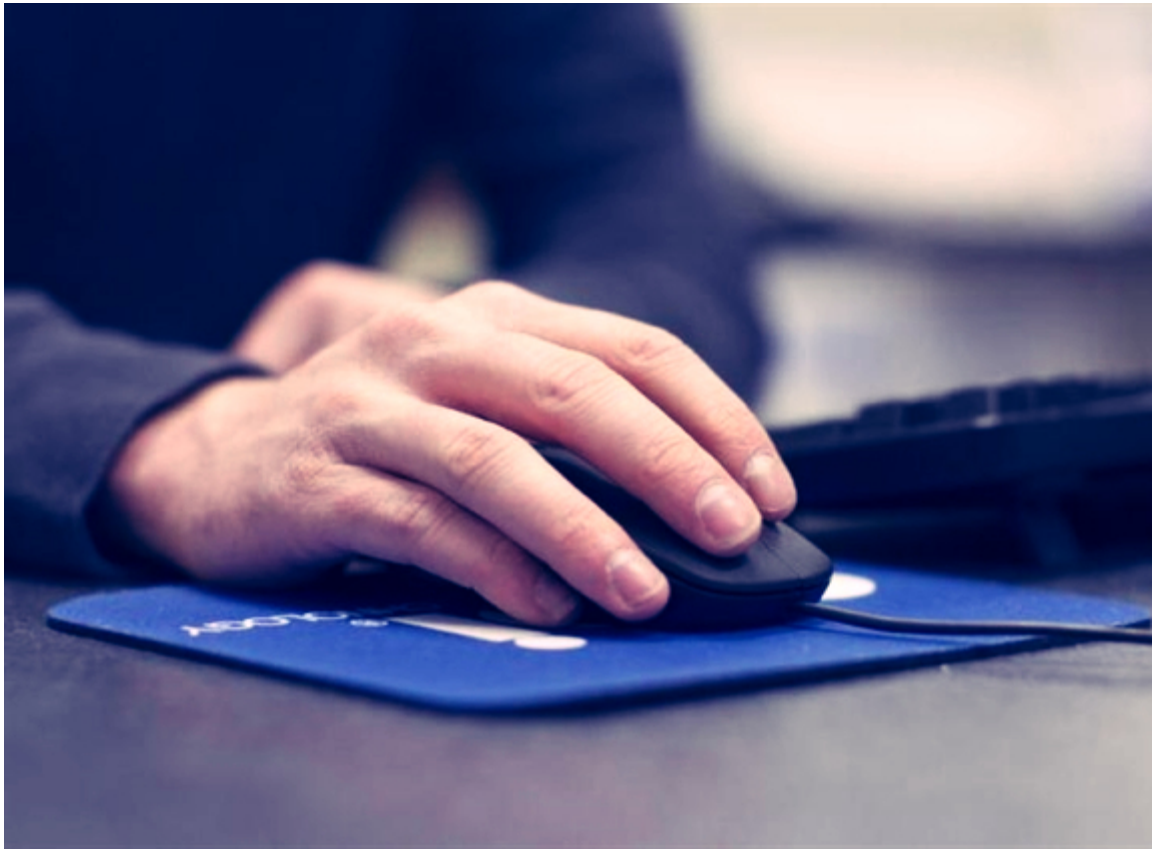
- Alacsony jogosult felhasználói account birtokában történik a vizsgálat.
- A cél magasabb felhasználói jogok megszerzése, a rendszer feltörése.

White box vizsgálat

- A rendszer felépítésről, architektúráról és komponensekről minden információ átadásra kerül, adott esetben privilegizált felhasználói account is.
- A cél ekkor nem a rendszer feltörése, hanem az architektúra és az alkalmazott technikai biztonsági kontrollok gyengeségeinek felderítése.

Sérülékenységvizsgálat módszertan

OWASP Top 10

- Beszúrásos típusú támadások
- Hibás hitelesítés és sessionkezelés
- Cross-Site Scripting
- Nem biztonságos direkt objektumhivatkozás
- Helytelen biztonsági beállítások
- Érzékeny adat nem megfelelő védelme
- Helytelen URL és függvény validáció
- Cross-Site Request Forgery (CSRF)
- Hibás beépülő komponensek használata
- Nem ellenőrzött átirányítások és továbbítások

Köszönöm a figyelmet!